Avocent®

MERGEPOINT® 52XX

Installer/User Guide

USA Notification

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Notification

This class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Safety and EMC Approvals and Markings for the MergePoint 5200 SP Manager

FCC Class B, EN 55022 Class B, EN 61000-3-2/-3-3, CISPR 22 Class B, EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11), EN 60950/IEC 60950-Compliant, UL Listed (USA), CUL Listed (Canada), TUV Certified (Germany), CE Marking (Europe)

Safety and EMC Approvals and Markings for the MergePoint 5224/5240 SPManager

FCC Class A; EN55022 Class A/CISPR 22 Class A; EN55024/CISPR 24 (EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN 61000-4-6, EN 61000-4-11); EN60950/IEC60950-Compliant; CSA Listed (USA and Canada); CE Marking (Europe)

MergePoint® Service Processor Manager 5200/5224/5240

Installer/User Guide

Avocent, the Avocent logo, The Power of Being There, MergePoint and DSView are registered trademarks of Avocent Corporation or its affiliates in the U.S. and other countries. All other marks are the property of their respective owners.

© 2008 Avocent Corporation. All rights reserved. 590-765-501B

Instructions

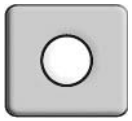
This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

Dangerous Voltage

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

Power On

This symbol indicates the principal on/off switch is in the on position.



Power Off

This symbol indicates the principal on/off switch is in the off position.

Protective Grounding Terminal

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

TABLE OF CONTENTS

List of Figures ..... **ix**

List of Tables ..... **xi**

Chapter 1: Product Overview **1**

Features and Benefits *1*
Supported Target Devices *2*
MergePoint 5200 Appliance Configuration *3*
LEDs on the MergePoint 5200 appliance *3*
MergePoint 5224/5240 Appliance Configuration *4*
Ports on the MergePoint 5224/5240 appliance *5*
LEDs on the MergePoint 5224/5240 appliance *6*

Chapter 2: Installation and Setup **7**

Safety Precautions *7*
Rack mount safety considerations *8*
Cabling installation, maintenance and safety tips *9*
Installing the MergePoint SP Manager *10*
Configuring power for the MergePoint SP manager *10*
Enabling Web Interface Access *12*
Configuring the MergePoint 5200 Appliance License Keys *13*
Adding the MergePoint SP Manager to a DSView 3 Software Installation *14*
Setting Up the MergePoint SP Manager Network *14*
Ethernet ports on the MergePoint 5200 appliance *14*
Ethernet ports on the MergePoint 5224/5240 appliance *14*
Configuring MergePoint 5200 appliance network settings *15*
Configuring MergePoint 5224/5240 appliance network settings *16*
Private Subnets on the MergePoint 5224/5240 Appliance *17*
Firewall/Packet Filtering *18*
Chains *18*
Rules *19*
BMC Provisioning (IPMI Targets Only) *20*
Starting or stopping the BMC provisioning service (Admin users only) *20*

Configuring PXE parameters for IPMI BMC provisioning (Admin users only) *20*
BMC log *21*
Users *22*
Managing MergePoint SP manager user accounts *22*
DHCP on the MergePoint SP Manager *24*
Discovering and Adding Target Devices (Admin users only) *25*
Discovering target devices *25*
Manually Adding a Single Target Device *26*
Managing Target Device Lists (Admin users only) *28*
Managing Target Device Groups (Admin users only) *30*
Managing SP Profiles (Admin users only) *31*
Managing Default Users (Admin users only) *33*
Managing user accounts on target devices *33*
Configuring the MergePoint SP Manager System *34*
System settings (Admin users only) *34*
PCMCIA for the MergePoint 5224/5240 Appliance *36*
Completing the MergePoint SP Manager Installation *37*

Chapter 3: Operations 39

Using the MergePoint SP Manager *39*
MergePoint SP manager web interface *39*
Power Management *41*
Remote power and chassis management *41*
Performing Target Device Group Operations *42*
Monitoring and Management *44*
Viewing sensor status *44*
Viewing SEL events *45*
Viewing the accounting log *45*
Import/export data *45*
Accessing FRU information *46*
Using the Alerts Viewer *46*
Syslog *48*
Configuring PET alerts *49*
Schedules *50*
Schedule a task (Admin users only) *50*

Target Operations *50*
Viewing target device information *51*
Synchronizing blades for a blade chassis *51*
Changing the SoL port number *51*
Changing the access account of a target device *52*
Changing target device parameters *52*
Accessing system information *53*
Recovering provisioning *53*
Changing LAN parameters *54*
SNMP *54*
Host table *57*
Static routes *58*
Using Serial over Lan (SOL) *58*
Device console and service processor console *58*
Configuring SoL parameters *61*
NFS *61*
Remote control *61*
Diagnostics *62*
DirectCommand *63*
Direct access to service processor applications through Native IP (MergePoint 5224/5240 appliances only) *65*
Appliance Operations *68*
MergePoint SP manager sessions *68*
Upgrade *68*
Boot configuration for MergePoint 5224/5240 appliance *69*
Unbinding the MergePoint SP manager from the DSView 3 server *70*

Chapter 4: Configuring External Authentication Services 71

Configuring Authentication Services *71*
Configuring a Kerberos authentication server *72*
Configuring an LDAP authentication server *73*
Configuring an NIS authentication server *74*
Configuring a RADIUS authentication server *74*
Configuring an SMB authentication server *75*
Configuring a TACACS+ authentication server *75*

Configuring an authentication method for the MergePoint SP manager *76*

Chapter 5: Administration Tasks Not Performed in the Web Interface 77

Using MindTerm to Create an SSH Tunnel *77*
Using SSH with the MergePoint SP Manager *78*
The SSH command line format *78*
User shell *79*
MgpShell *80*
SSH Commands for Native IP *80*
SSH Passthrough *82*
SSH Passthrough commands *82*
Telnet *83*
Configuring the Users' Console Login Menu *84*
Configuring Routes With CLI *85*
Backing Up Configuration Files *86*
Restoring backed up configuration files *86*
Restoring factory default configuration files *87*
Configuring Groups for Use with Authentication Servers *87*
Configuring group authorization for LDAP authentication *87*
Configuring group authorizations on an AD server *88*
Defining groups on an LDAP server running OpenLDAP *89*
Configuring group authorization for RADIUS authentication *90*
Configuring group authorization for TACACS+ authentication *93*
Switching the Port Speed in the MergePoint 5224/5240 Appliance *95*

Chapter 6: Using the CLI Utility 97

CLI Utility Overview *97*
Execution Modes *97*
Command line mode *97*
Interactive mode *98*
Batch mode *98*
CLI Options *98*
CLI Parameters and Arguments *99*
Entering a command in interactive mode *99*
Entering a command in command code *100*
Entering a command in batch mode *100*

Autocompletion *101*
CLI Commands *102*
add *102*
cd *106*
commit *107*
delete *107*
get | show *108*
list *109*
quit | exit *109*
quit! *109*
rename *110*
revert *110*
set *111*
shell *111*
version *111*
Summary of How to Configure the Top Level Parameters *112*
Appendices **121**
Appendix A: Troubleshooting *121*
Appendix B: Technical Specifications *124*
Appendix C: Access Privileges *126*
Appendix D: Configuring the BIOS Settings for SoL *129*
Appendix E: Configuring a Virtual Serial Port *130*
Appendix F: Profile Configuration *131*
Appendix G: Advanced Boot and Backup Configuration *141*
Appendix H: Reserved Words *145*
Appendix I: Glossary and Acronyms *146*
Appendix J: Technical Support *148*
License Information **149**

LIST OF FIGURES

Figure 1.1: MergePoint 5200 Appliance Configuration *3*
Figure 1.2: MergePoint 5224/5240 Appliance Configuration *4*
Figure 1.3: MergePoint SP Manager with Ethernet, AUX and Console Ports *5*
Figure 1.4: LEDs for Public and Private Ethernet Ports, AUX and Console Ports (Front) *6*
Figure 2.1: DC Power Connection Terminal Block *11*
Figure 3.1: MergePoint 5200 Appliance Web Interface *40*
Figure 3.2: MergePoint 5224/5240 SP Manager Native IP Configuration *66*
Figure 5.1: MindTerm Basic Tunnels Setup Dialog Box *78*
Figure G.1: Partitions Layouts *141*

LIST OF TABLES

Table 1.1: Descriptions for MergePoint 5200 Appliance Configuration *3*
Table 1.2: Descriptions for MergePoint 5224/5240 Appliance Configuration *4*
Table 1.3: Descriptions for MergePoint SP Manager Ethernet, AUX and Console Ports *5*
Table 1.4: Descriptions for MergePoint SP Manager Ethernet, AUX and Console Ports *6*
Table 2.1: DC Power Connection Details *11*
Table 2.2: Target Device Types Displayed in the Managed/Unmanaged Targets Lists *28*
Table 3.1: MergePoint 5200 Appliance Web Interface Descriptions *40*
Table 3.2: Descriptions for MergePoint 5224/5240 SP Manager Native IP Configuration *66*
Table 4.1: Supported Authentication Methods *71*
Table 5.1: Supported Service Processor Commands *82*
Table 6.1: CLI Utility Options *98*
Table 6.2: Parameters that Work with the CLI add Command *104*
Table 6.3: Setting Top Level CLI Parameters *112*
Table B.1: MergePoint 5200 Appliance Technical Specifications *124*
Table B.2: MergePoint 5224/5240 Appliance Specifications *125*
Table F.1: Default Family Names and Corresponding Expect Script Names *132*
Table F.2: Expect Script Exit Codes *133*
Table F.3: Default Command Templates *136*
Table H.1: Reserved Words *145*

CHAPTER 1

Product Overview

The MergePoint service processor (SP) manager is a secure, centralized enterprise management solution for target devices equipped with IPMI, HP®, Dell®, IBM®, Sun® and Fujitsu-Siemens service processors. You can remotely perform server management tasks, including power control and console access, on managed target devices.

The MergePoint SP manager provides a standardized interface independent of the management protocols used to manage each target device. Management operations can be performed using the following three methods:

- The DSView® 3 management software interface.
- The MergePoint SP manager web interface from a standard web browser.
- Commands or scripts over a Telnet, command line interface (CLI) utility, or Secure Shell (SSH) session.

  The CLI utility provides a single command line interface to manage servers from multiple manufacturers, simplifying management and streamlining interoperability while providing scripting and automation capabilities.

NOTE: MergePoint SP manager refers to the 5200/5224/5240 models. For features supported only by some models, the supported model is noted.

Features and Benefits

The MergePoint 52XX SP manager provides secure Serial over LAN (SoL) console access, power control and server hardware monitoring. With easy-to-use IPMI provisioning capabilities and an auto discovery mechanism for server management technologies within the network, the MergePoint appliance is ideal for enterprise data centers as well as for high performance computing (HPC) and other clustering environments.

The MergePoint appliance allows enterprise-class authentication, authorization and auditing (AAA) security and encryption, and extends this functionality to all servers. Other standard features include data logging, event detection and notification, SNMP proxy, graphing and alarm events for sensors and shared access to management ports. Also, simultaneous power control of

multiple servers boosts the already existing power management capabilities of service processors, including graceful shutdown support for IPMI.

The DirectCommand management option provides native access to target devices and enables users to connect directly to the web management interface or command line of a target device. With this feature, users can gain access to native applications, integrated web servers and other proprietary interfaces that are available over IP. Alternatively, for target devices that do not support DirectCommand, the MergePoint 5224/5240 appliance Native IP feature allows transparent access to the native applications on the service processor. Examples of native applications include HP Insight, IBM Director and Dell Open Manage®.

Supported Target Devices

The MergePoint SP manager supports target devices with a variety of service processors, including:

- IPMI (Intelligent Platform Management Interface) 1.5 and 2.0

NOTE: The IPMI service processor is also referred to as a baseboard management controller (BMC).

- Dell DRAC (Dell Remote Access Card) 3, 4 and 5
- Dell 10G
- Dell DRAC/MC (Remote Access Controller/Modular Chassis)
- Hewlett Packard (HP) iLO (Integrated Lights-Out) and iLO 2
- HP IPMI
- HP BladeSystem c-Class
- IBM BladeCenter E Chassis
- IBM BladeCenter H Chassis
- IBM RSA (Remote Supervisor Adapter) II
- Sun ILOM (Integrated Lights Out Management)
- Sun ALOM (Advanced Lights Out Management)
- FSC iRMC (Fujitsu-Siemens Corp integrated Remote Management Card)

Additionally, administrators can configure new target devices or modify existing target device types for service processors not included in the previous list. For a complete list of supported service processors, see the MergePoint SP manager release notes.

MergePoint 5200 Appliance Configuration

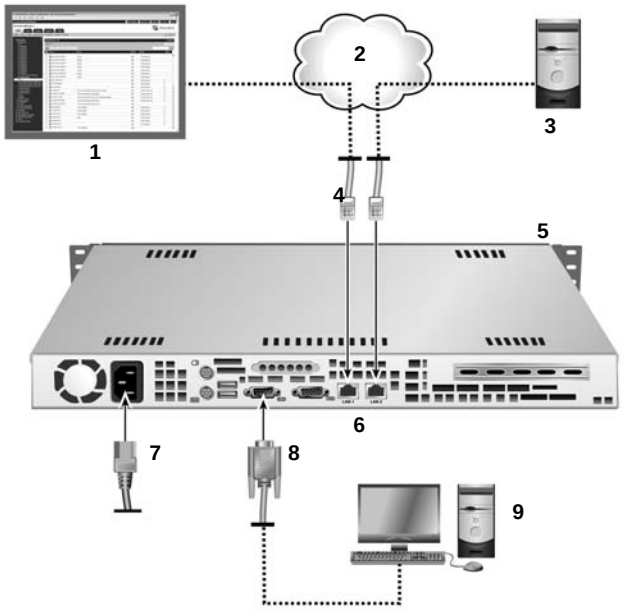


Figure 1.1: MergePoint 5200 Appliance Configuration

Table 1.1: Descriptions for MergePoint 5200 Appliance Configuration

Number	Description	Number	
1	Remote User Web Interface	**6**	RJ-45 Ethernet Ports
2	LAN	**7**	Power
3	Target Device	**8**	Connection to the Serial Port
4	CAT 5 Cables	**9**	Terminal or Workstation (for Configuration)
5	MergePoint 5200 Appliance		

LEDs on the MergePoint 5200 appliance

On the front of the MergePoint 5200 appliance, the LAN LED provides information about the LAN activity; the LED blinks to indicate activity. The power LED is green if the MergePoint 5200 appliance is turned on.

MergePoint 5224/5240 Appliance Configuration

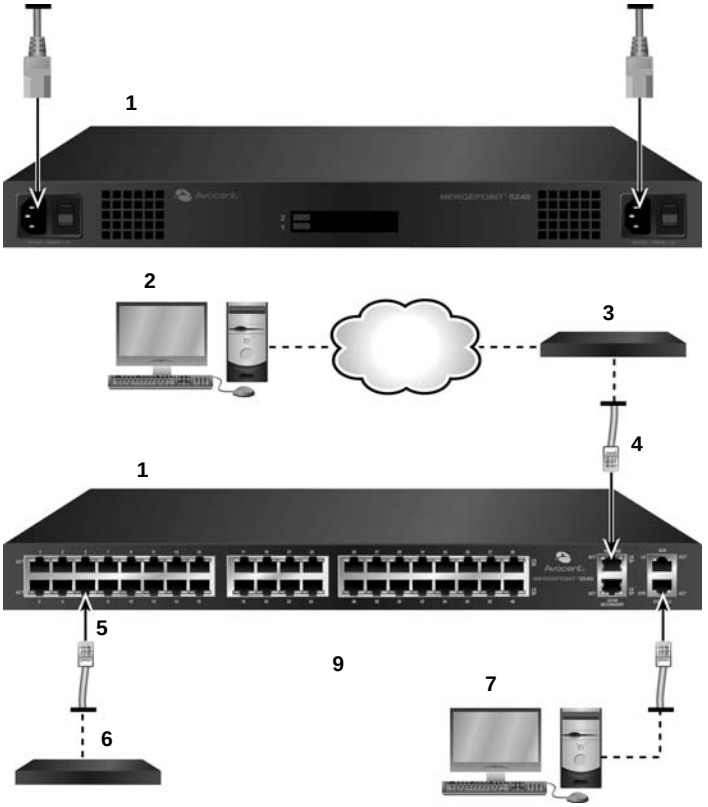


Figure 1.2: MergePoint 5224/5240 Appliance Configuration

Table 1.2: Descriptions for MergePoint 5224/5240 Appliance Configuration

Number	Description
1	MergePoint 5224/5240 Appliance
2	Remote User Web Interface
3	Ethernet
4	CAT 5 Cables
5	RJ-45 Ethernet Ports
6	Blade or Service Processor
7	Console User

Ports on the MergePoint 5224/5240 appliance

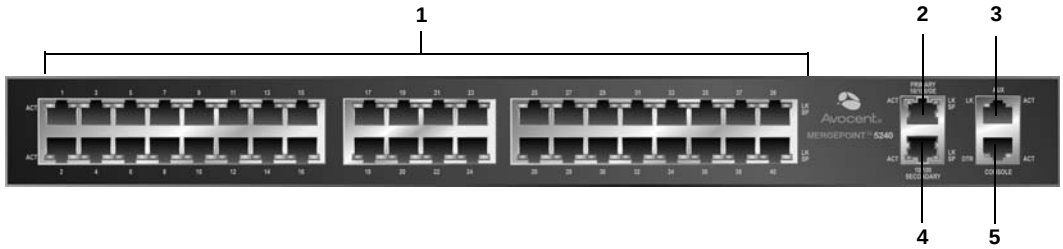


Figure 1.3: MergePoint SP Manager with Ethernet, AUX and Console Ports

Table 1.3: Descriptions for MergePoint SP Manager Ethernet, AUX and Console Ports

Number	Type	Purpose
1	Private Ethernet ports, either 24 or 40	For connecting service processors and other devices that have dedicated Ethernet ports for management access
2	10/100/GE (Gigabit Ethernet) primary public Ethernet port	For network connection
3	Auxiliary (AUX) port	Disabled
4	10/100 secondary public Ethernet port	(Optional) For connection to a second network connection or for failover connection to the primary network; with Ethernet failover (also known as bonding) enabled, if the primary Ethernet port fails, the secondary one automatically becomes active until the first one recovers
5	Console port	For connecting either a terminal or a computer running a terminal emulation program to enable local administrators and users to access the command line

LEDs on the MergePoint 5224/5240 appliance

Two LEDs on each port provide status information about the ports.

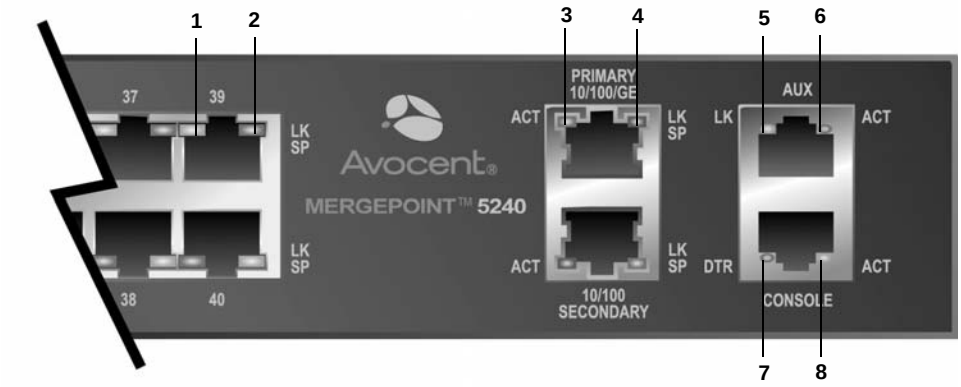


Figure 1.4: LEDs for Public and Private Ethernet Ports, AUX and Console Ports (Front)

Table 1.4: Descriptions for MergePoint SP Manager Ethernet, AUX and Console Ports

Number	Label	Function	Color/Status
1, **3** (the left LED on all Ethernet ports)	ACT	Monitor Ethernet activity	OFF – Indicates no activity. Green – Blinks for any activity.
2, **4** (the right LED on all Ethernet ports)	LK/SP	Monitor Ethernet link and speed	OFF – Indicates either link is not up or cable is not connected. Green – Indicates the speed is 100 or 1000 Megabits/second. Yellow – Indicates the speed is 10 Megabits/second.
5	LK	Monitor RS232 link	OFF – Indicates either link is not up or cable is not connected. Green – Lights solid when the link is up and blinks when activity occurs, with frequency proportional to traffic.
6, **8**	ACT	Monitor RS232 async activity	OFF – Indicates no data activity. Green – Blinks when data is either being received (RX) or transmitted (TX).
7	DTR	Monitor console port for transmissions	OFF – Indicates the MergePoint SP manager is not ready to communicate. ON – Indicates the MergePoint SP manager is ready to communicate.

CHAPTER 2

Installation and Setup

The installation of a MergePoint SP manager consists of the following steps:

- Connecting power
- Connecting to the network
- Connecting service processors
- Basic configuration of the MergePoint SP manager
- Adding and configuring service processors within the MergePoint SP manager
- Final configuration of the MergePoint SP manager

Safety Precautions

To avoid potentially fatal shock hazard and possible damage to equipment, please observe the following precautions:

- Do not use a 2-wire power cord in any Avocent product configuration.
- Test AC outlets at the target device and monitor for proper polarity and grounding.
- Use only with grounded outlets.

NOTE: The AC inlet is the main power disconnect.

Failure to observe the precautions in this section may result in personal injury or damage to equipment.

Observe the following general safety precautions when setting up and using Avocent equipment.

- Follow all cautions and instructions marked on the equipment.
- Follow all cautions and instructions in the installation documentation or on any cautionary cards shipped with the product.
- Do not push objects through the openings in the equipment. Dangerous voltages may be present. Objects with conductive properties can cause fire, electric shock or damage to the equipment.
- Do not make mechanical or electrical modifications to the equipment.
- Do not block or cover openings on the equipment.

- Choose a location that avoids excessive heat, direct sunlight, dust or chemical exposure, all of which can cause the product to fail. For example, do not place an Avocent product near a radiator or heat register, which can cause overheating.
- Connect products that have dual power supplies to two separate power sources, for example, one commercial circuit and one uninterruptible power supply (UPS). The power sources must be independent of each other and must be controlled by separate circuit breakers.
- For products that have AC power supplies, ensure that the voltage and frequency of the power source match the voltage and frequency on the label on the equipment.
- Products with AC power supplies have grounding-type three-wire power cords. Make sure the power cords are plugged into single-phase power systems that have a neutral ground.
- Do not use household extension power cords with Avocent equipment because household extension cords are not designed for use with computer systems and do not have overload protection.
- Make sure to connect DC power supplies to a grounded return.
- Ensure that air flow is sufficient to prevent extreme operating temperatures. Provide a minimum space of 6 inches (15 cm) in front and back for adequate airflow.
- Keep power and interface cables clear of foot traffic. Route cables inside walls, under the floor, through the ceiling or in protective channels or raceways.
- Route interface cables away from motors and other sources of magnetic or radio frequency interference.
- Stay within specified cable length limitations.
- Leave enough space in front and back of the equipment to allow access for servicing.

When installing Avocent equipment in a rack or cabinet, observe the following precautions:

- Ensure that the floor’s surface is level.
- Load equipment starting at the bottom first and fill the rack or cabinet from the bottom to the top.
- Exercise caution to ensure that the rack or cabinet does not tip during installation and use an anti-tilt bar.

When using a desk or table, observe the following precautions:

- Choose a desk or table sturdy enough to hold the equipment.
- Place the equipment so that at least 50% of the equipment is inside the table or desk’s leg support area to avoid tipping of the table or desk.

Rack mount safety considerations

- Elevated Ambient Temperature: If installed in a closed rack assembly, the operating temperature of the rack environment may be greater than room ambient. Use care not to exceed the rated maximum ambient temperature of the switch.

- Reduced Air Flow: Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- Mechanical Loading: Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Consider equipment nameplate ratings for maximum current.
- Reliable Earthing: Reliable earthing of rack mounted equipment should be maintained. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

Cabling installation, maintenance and safety tips

The following is a list of important safety considerations that should be reviewed prior to installing or maintaining your cables:

- Keep all CAT 5 runs to a maximum of 10 meters each.
- Maintain the twists of the pairs all the way to the point of termination, or no more than one half inch untwisted. Do not skin off more than one inch of jacket while terminating.
- If bending the cable is necessary, make it gradual with no bend sharper than a one inch radius. Allowing the cable to be sharply bent or kinked can permanently damage the cable's interior.
- Dress the cables neatly with cable ties, using low to moderate pressure. Do not overtighten ties.
- Cross-connect cables where necessary, using rated punch blocks, patch panels and components. Do not splice or bridge cable at any point.
- Keep CAT 5 cable as far away as possible from potential sources of EMI, such as electrical cables, transformers and light fixtures. Do not tie cables to electrical conduits or lay cables on electrical fixtures.
- Always test every installed segment with a cable tester. "Toning" alone is not an acceptable test.
- Always install jacks so as to prevent dust and other contaminants from settling on the contacts. The contacts of the jack should face up on the flush mounted plates, or left/right/down on surface mount boxes.
- Always leave extra slack on the cables, neatly coiled in the ceiling or nearest concealed location. Leave at least five feet at the work outlet side and 10 feet at the patch panel side.
- Choose either 568A or 568B wiring standard before beginning. Wire all jacks and patch panels for the same wiring scheme. Don't mix 568A and 568B wiring in the same installation.
- Always obey all local and national fire and building codes. Be sure to firestop all cables that penetrate a firewall. Use plenum rated cable where it is required.

CAUTION: This MergePoint SP manager contains an internal battery that is used for the real time clock. This battery is not a field replaceable item, and replacement should not be attempted by a user. If real time clock errors occur and the battery is suspected, visit http://www.avocent.com/support or contact the Avocent Technical Support location nearest you.

WARNING: For Service Personnel Only - There is a risk of explosion if the battery is replaced with an incorrect type. Dispose of used batteries according to the manufacturer's instructions.

Installing the MergePoint SP Manager

To connect and turn on the MergePoint SP manager:

1. Rack mount or place the MergePoint SP manager at the top of your server rack.
2. For a MergePoint 5200 appliance: Using Ethernet cables, connect the LAN1 (eth0) network port on the back of the appliance to the external network, and connect the LAN2 (eth1) port to the internal network. In a typical installation, the LAN1 port provides access to the web interface, and the LAN2 port provides access to the service processors.

   -or-

   For a MergePoint 5224/5240 appliance: Connect an Ethernet cable from the primary Ethernet 10/100/GE (Gigabit Ethernet) port to the network. If desired, connect an Ethernet cable to the secondary Ethernet 10/100 port and configure the port for failover (see *Configuring MergePoint 5224/5240 appliance network settings* on page 16).

   Connect an Ethernet cable from any private Ethernet port on the MergePoint 5224/5240 to dedicated Ethernet ports on a service processor or a dedicated Ethernet port on a blade server that manages multiple blade service processors.

NOTE: Service processors should be configured according to their manufacturer's instructions.

Configuring power for the MergePoint SP manager

The MergePoint SP manager is supplied with single or dual AC or DC power supplies.

To configure AC power:

1. Make sure that the power switch on the MergePoint SP manager is turned off.
2. Plug the power cable into the MergePoint SP manager and into a power source.
3. Turn the MergePoint SP manager on.
4. Turn on the power switches of the connected devices.

To configure DC power:

DC power is connected to DC-powered MergePoint SP managers by way of three wires: Return (RTN), Ground (GND) and -48VDC.

WARNING: It is critical that the power source supports the DC power requirements of your appliance. Make sure that your power source is the correct type and that your DC power cables are in good condition before proceeding. Failure to do so could result in damage to the equipment or in personal injury.

The following diagram shows the connector configuration for connecting DC power. You may use either a flat-blade or Phillips screwdriver for this procedure.

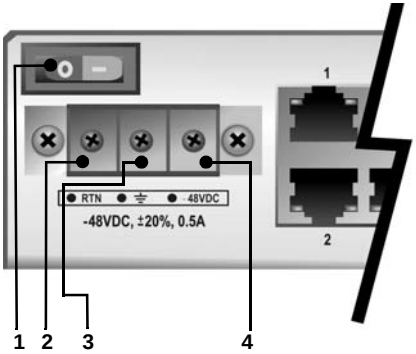


Figure 2.1: DC Power Connection Terminal Block

Table 2.1: DC Power Connection Details

Number	Description
1	Power switch
2	RTN (Return)
3	GND (Ground)
4	-48VDC

1. Make sure that the power switch on the console server is turned off.
2. Make sure that DC power cables are not connected to a power source.
3. Remove the protective cover from the DC power block by sliding it to the left or right.
4. Loosen all three DC power connection terminal screws.
5. Connect your return lead to the RTN terminal and tighten the screw.
6. Connect your ground lead to the GND terminal and tighten the screw.
7. Connect your -48VDC lead to the -48VDC terminal and tighten the screw.
8. Slide the protective cover back into place over the DC terminal block.
9. If your MergePoint SP manager has dual-input DC terminals, repeat steps 3 - 8 for the second terminal.
10. Connect the DC power cables to the DC power source and turn on the DC power source.

11. Turn on the MergePoint SP manager.
12. Turn on the power switches of the connected devices.

Enabling Web Interface Access

Before a MergePoint appliance can be added to your network, it must have an IP address to identify it. By default, it is DHCP enabled and can obtain an IP address from an available DHCP server.

For installations where a DHCP server is unavailable or not desired, the IP address can be assigned through a serial connection.

To configure the MergePoint SP manager IP address through a serial connection:

1. Connect a terminal or a workstation that is running a terminal emulation program to the serial port.
2. Start a session with the port settings of serial speed as 9600 bps, data length as 8 data bits, parity as none, stop bits as 1, flow control as none and emulation as ANSI.

   Once a connection is established, a prompt appears.
3. For the MergePoint 5200 appliance:
   a. Type **2** (Network Config).
   b. Type **1** (Setup eth) to configure any of the listed network settings specific to your network.

   -or-

   For a MergePoint 5224/5240 appliance:

   a. Log into the console port as **root** with the default password **avocent**.
   b. Enter the **passwd** command, and enter and confirm a new password for the root user.
   c. Type **cli** to load the CLI utility.
   d. Configure the primary Ethernet interface (eth0) by setting the method to static and assigning a static IP address, a gateway and a netmask:

      ```
      cli> set network interface eth0 method static address
      <SPmanager_IPaddress> gateway <gateway_IP_address> netmask
      <netmask>
      ```

   e. Specify a hostname, a domain, a DNS server IP address, and an optional secondary DNS server IP address:

      ```
      cli> set network hostname <appliance_name> resolv domain
      <domain_name> dns0 <DNS_server_IPaddress> dns1
      <secondary_DNS_server_IPaddress>
      ```

   f. Confirm the configuration for the interface:

      ```
      cli> get network interface eth0
      ```

   g. Confirm the name server configuration:

```
cli> get network resolv
```

h. Save the changes:

```
cli> commit
```

i. Exit from the CLI utility:

```
cli> quit
```

NOTE: To restore default configuration parameters, type **restorefactory.** To restart the MergePoint SP manager using a previous firmware version, type **roll_back.sh**.

NOTE: For more information on configuring IP address, see *Summary of How to Configure the Top Level Parameters* on page 112.

Configuring the MergePoint 5200 Appliance License Keys

You must register your MergePoint 5200 appliance online at www.avocent.com to obtain a master license key. The master key must be configured before you can discover and manage any target devices. The license included with your MergePoint 5200 appliance allows you to discover and manage up to 64 target devices.

NOTE: Registration is not required for the MergePoint 5224/5240 appliance.

A license key is made up of a master key and a slave key(s). The master key is used to activate the MergePoint 5200 appliance and its slave keys specify the number of managed target devices that are supported by the license.

You may purchase upgrade licenses to add support for additional target devices up to a maximum of 256. If you purchase one or more upgrade licenses, perform the procedures below to configure the MergePoint 5200 appliance with the master key and slave key(s) for the new license key(s).

To activate the MergePoint 5200 appliance license:

1. Follow the instructions on the registration card included with the MergePoint 5200 appliance to activate the appliance serial number. Once completed, you will receive a master license key.
2. Open a web browser and enter the IP address (**http://<appliance IP address>**) of the appliance.
3. The MergePoint 5200 appliance web interface window appears. Type the master key in the fields provided and click *Add*.
4. The User Login window appears. Type **admin** as the username and type **admin** as the password. To change the admin password, see *To add an appliance user (Admin users only):* on page 22.

To view license information (Admin users only):

5. Click *System – Licenses* for a license summary and list of license keys and descriptions.

To add a master or slave key:

1. Click the *System* tab.
2. In the top navigation bar, click *Licenses*. The License window appears.
3. Click *Add Master Key* or *Add Slave Key* and type the master key.
4. Click *Apply.*

Adding the MergePoint SP Manager to a DSView 3 Software Installation

If you will be using the MergePoint SP manager within a DSView 3 software installation, you may now use the DSView 3 software Add Appliance wizard to add the MergePoint SP manager and finish configuration. For detailed instructions, refer to the DSView 3 software installer/user guide.

Setting Up the MergePoint SP Manager Network

Ethernet ports on the MergePoint 5200 appliance

The MergePoint 5200 appliance has two public Ethernet ports (eth0 and eth1), which are labeled LAN1 and LAN2. The eth0 port is for connecting to the external network and eth1 is for connecting to service processors on the internal network.

NOTE: Connecting service processors to eth0 is not recommended because some services, like BMC provisioning or DHCP servers, only listen to eth1.

Ethernet ports on the MergePoint 5224/5240 appliance

The MergePoint 5224/5240 appliance has two public Ethernet ports (eth0 and eth1) and 24 or 40 Ethernet private ports. The public ports are used for connecting to the public (or management) network and the private ports are used for connecting to service processors on the private network. Therefore, the managed private side of the MergePoint SP manager is isolated from the public side to ensure security. Access to all connected service processor servers is consolidated through the one publicly known IP address.

Private Ethernet ports

The MergePoint 5224/5240 appliance is aware of only a single interface to the private network, priv0, for communicating with the target devices. Packets are sent and received by priv0 through the private Ethernet ports.

Each private Ethernet port may be connected to one or to multiple service processors. For example, an Ethernet port may be connected to a blade manager with multiple service processors, and in those cases a single private Ethernet port may require multiple IP addresses.

All communication among private Ethernet ports is blocked unless priv0 is the sending or receiving port.

Public Ethernet ports

On the public side of the MergePoint 5224/5240 appliance, the primary and secondary Ethernet ports are referred to as eth0 and eth1.

Failover

Failover is important for high-availability environments where constant accessibility is required to support mission-critical applications. The secondary Ethernet port on the MergePoint 5224/5240 appliance can optionally be configured for failover. Failover automatically redirects traffic from the primary Ethernet port to the secondary Ethernet port should the primary interface fail.

The primary Ethernet port continues to be monitored, and when it starts functioning again, traffic is then automatically redirected back through the primary Ethernet port. All connection sessions continue without interruption.

With failover, both the primary and secondary Ethernet ports are assigned a single IP and single MAC [Ethernet] address. After failover is enabled, the bonded Ethernet interfaces are referred to as bond0.

Bridge mode

Bridge mode bridges the private Ethernet ports with the public Ethernet ports, allowing traffic to go through the MergePoint 5224/5240 appliance from a host on the external network to a service processor on the internal network and vice-versa, with no interference from the MergePoint SP manager itself.

After Bridge mode is enabled, the bridged Ethernet interfaces are referred to as br0; the eth0, eth1 and priv0 are not accessible at the same time.

NOTE: If Bridge mode is enabled, security settings are no longer managed by the MergePoint SP manager. Instead, the user must configure any required security settings from the service processor attached to the MergePoint SP manager.

Configuring MergePoint 5200 appliance network settings

In the Appliance Network Setting window, you can set IP addresses for the Ethernet ports and configure a DNS server.

A primary and a secondary DNS server may be configured to allow the use of target device names instead of IP addresses.

You can also set VLAN for each Ethernet interface.

To configure network settings for the MergePoint 5200 appliance (Admin users only):

1. Click the *Network* tab.
2. In the top navigation bar, click *Network*.
3. Select *Eth0* or *Eth1* as the default gateway and click *Apply.*

4. Configure the following fields for the Domain Name System (DNS) server:
   a. In the Primary server field, type the IP address of the primary server.
   b. In the Secondary server field, type the IP address of the secondary server.
   c. In the Domain name field, type the domain name.
   d. Click *Apply*.
5. Click a device link. Configure IPv4 and/or IPv6 addresses by entering the following information in the respective areas.
   a. In the MTU field, accept or change the existing value.
   b. For the DHCP method, select *DHCP*.

      -or-

      For the Static method, select *Static* and enter the address, subnet mask, gateway in the fields provided. For IPv4 only, also enter the broadcast in the field provided.

   c. Click *Apply*.

To enable VLAN for the MergePoint 5200 appliance (Admin users only):

1. Click the *Network* tab.
2. Click a device link. Configure VLAN for the device:
   a. In the ID field, type the ID for the VLAN.
   b. In the Status drop-down menu, select *Yes* to enable VLAN.
   c. Click *Apply*.

Configuring MergePoint 5224/5240 appliance network settings

When configuring Ethernet ports, be aware of the following conditions:

- In Normal mode, when each Ethernet port is active and assigned a different IP address, both ports are reachable through either IP address even if the cable is disconnected from one of the interfaces.
- In Failover mode, the secondary Ethernet interface becomes bonded to the primary Ethernet interface and both are referred to as a single bond0 interface. As a result, the same set of values applies to the single bond0 interface.
- In Bridge mode, both the primary and secondary Ethernet interface become disabled. In addition, security settings are no longer managed by the MergePoint SP manager. Instead, the user must configure any required security settings from the service processor attached to the MergePoint SP manager.

To configure network settings for the MergePoint 5224/5240 appliance (Admin users only):

1. Click the *Network* tab.
2. In the top navigation bar, click *Network*. The Appliance Network Setting window appears.

3. In the mode drop-down menu, select the mode and click *Apply.*
4. Select *eth0* or *eth1* as the default gateway and click *Apply.*
5. Configure the following fields for the Domain Name System (DNS) server:
   a. In the Primary server field, type the IP address of the primary server.
   b. In the Secondary server field, type the IP address of the secondary server.
   c. In the Domain name field, type the domain name.
   d. Click *Apply*.
6. Click a device link. Configure IPv4 and/or IPv6 addresses by entering the following information in the respective areas.
   a. In the MTU field, accept or change the existing value.
   b. For the DHCP method, select *DHCP*.

      -or-

      For the Static method, select *Static* and enter the address, subnet mask, gateway in the fields provided. For IPv4 only, also enter the broadcast in the field provided.

   c. Click *Apply*.

NOTE: For Normal mode, you may configure either eth0 or eth1, or both. For Failover mode, you only need to configure Ethernet port bond0. For Bridge mode, you only need to configure Ethernet port br0.

NOTE: Network settings may also be changed using the CLI utility. See related CLI commands on *page 114*.

Private Subnets on the MergePoint 5224/5240 Appliance

Target devices connecting to the private subnets on a MergePoint 5224/5240 appliance can be isolated on a management network that is separate from the production and public networks. To enable communications between the target devices and the MergePoint 5224/5240 appliance, an Admin user must configure at least one private subnet. The Admin user then assigns each private subnet the following:

- A name
- An address within the private subnet's address range to be used by the target device when communicating with the MergePoint SP manager

Any number of private subnets may be configured. Multiple private subnets may be needed if IP addresses for target devices are not in the same range.

NOTE: If changing or deleting a private subnet, reassign all affected devices to another private subnet to avoid making them unavailable.

To add a private subnet:

1. Click *Network - Private subnet.*

2. Click *Add*.
3. Enter a name in the Private subnet name field.
4. In the Appliance side IP address field, enter an IP address for the MergePoint 5224/5240 appliance within the private subnet's network address range.
5. In the Subnet Mask field, enter a netmask for the private subnet.
6. Click *Apply.*

To edit a private subnet:

1. Click *Network - Private subnet.*
2. Click the name link of the private subnet you want to edit.
3. Modify the fields as needed.
4. Click *Apply.*

To delete a private subnet:

1. Click *Network - Private subnet.*
2. Check the private subnet you want to delete and click *Delete*.

Firewall/Packet Filtering

Packet filtering on the MergePoint SP manager is controlled by chains and rules that are configured in iptables. By default, the MergePoint SP manager does not forward any traffic between private and public networks. Rules can be added to allow limited communications between specific target devices on the private network and the public network.

NOTE: It is possible for an Admin user to create rules that circumvent the access controls on a target device.

Chains

A chain is a type of named profile that defines rules for sorting packets.

The MergePoint SP manager has a number of built-in chains with hidden rules that are preconfigured to control communications between target devices connected to the private Ethernet ports and devices on the public side of the MergePoint SP manager.

The default chains are defined in filter and NAT (network address translation) iptables. The mangle table is not used. The built-in chains are named according to the type of packets they handle. The first three chains, INPUT, OUTPUT and FORWARD are in the iptables filter table.

PREROUTING, POSTROUTING and OUTPUT are in the NAT table and implement NAT. This includes redirecting packets addressed to a virtual IP to the target device's real IP address and then hiding the target device's real IP address when the target device sends packets to a user.

Rules

Each chain can have one or more rules that define the following:

- The packet characteristics being filtered. The packet is checked for characteristics defined in the rule, for example, a specific IP header, input and output interfaces and protocol.
- What action is performed when the packet characteristics match the rule. The packet is handled according to the specified action (called a Rule Target, Target Action or Policy).

Rules are listed in order of priority. You can change the rule order by clicking the arrow on the rule line. The arrow appears when there are at least two rules in a list.

When a packet is filtered, its characteristics are compared against each rule in the list until a match is found. Once a match is found, the packet is processed and no attempt is made to match lower priority rules.

To add a new packet filtering (firewall) rule:

1. Click *Network - Firewall*.
2. Click *Add* for the chain to which you wish to add a rule.
3. Configure one or more of the following filtering options, as desired.
   a. In the Protocol drop-down menu, select a protocol.
   b. In the Source IP/mask field, type a source IP and subnet mask in the form: hostIPaddress or networkIPaddress/NN.
   c. In the Destination IP/mask field, type a destination IP and subnet mask in the form: hostIPaddress or networkIPaddress/NN.
   d. In the Input interface or Output interface drop-down menu, select an input or output interface depending on which chain you select.
   e. In the Fragments drop-down menu, choose the type of packets to be filtered.
   f. In the Rule target drop-down menu, select a target.
4. Click *Apply.*

To edit a packet filtering (firewall) rule:

1. Click *Network - Firewall*.
2. Select the rule you want to change.
3. Modify the fields as needed.
4. Click *Apply.*

To delete a packet filtering (firewall) rule:

1. Click *Network - Firewall*.
2. Select the rule you want to delete and click the corresponding *Delete* button.

NOTE: Rules may also be changed using the CLI utility. See related CLI commands on *page 113*.

BMC Provisioning (IPMI Targets Only)

The default status of the BMC on a target device is disabled and should be provisioned before it can be discovered by the MergePoint SP manager.

The MergePoint SP manager provides a PXE (Preboot Execution Environment) based solution for provisioning the BMC and can be configured to automatically provision the IPMI BMC of a target device.

There are two modes of provisioning available: dynamic and static. For static provisioning, when the SP manager receives a PXE request from a target device, it can obtain its MAC address from the request and use it for comparison with the MAC address and IP address pairs in the static provisioning table. If a MAC address in the table meets this request, the MergePoint SP manager will assign the corresponding IP address to the target device.

Dynamic provisioning occurs when no match is found and the MergePoint SP manager selects an IP address from a specified range for the target device.

Once you have provisioned the BMC successfully, the target device is automatically initialized with the specified provisioning parameters and added to the Managed Targets list and side navigation bar where it can then be accessed with the MergePoint SP manager.

NOTE: Automatic provisioning is an optional feature that is only available for target devices that have IPMI BMCs.

Starting or stopping the BMC provisioning service (Admin users only)

You may start or stop the BMC provisioning service through the Provisioning window. If the *Stop* button is clicked, the BMC provisioning service stops and the MergePoint SP manager will no longer accept PXE boot requests from target devices on the LAN. However, previously provisioned target devices that have IPMI BMCs can still be discovered.

To stop or start the BMC provisioning service:

1. Click *Targets - Provisioning*.
2. In the Provisioning window, click *Stop* or *Start* as appropriate.

Configuring PXE parameters for IPMI BMC provisioning (Admin users only)

You must configure provisioning parameters for a BMC that will be initialized and managed by the MergePoint SP manager.

To set basic provisioning parameters in the MergePoint 5200 appliance:

1. Click *Targets - Provisioning*.
2. Enter the username and gateway address in the fields provided.
3. In both the Password and Confirm Password fields, enter the password.

4. Check the VLAN Enable field if you need to use VLAN on BMC, and specify the following VLAN parameters:
   a. In the VLAN ID field, type the VLAN ID.
   b. In the VLAN Priority field, type the VLAN priority.
5. Click *Apply*.

NOTE: For the MergePoint 5200 appliance, it is strongly recommended that the VLAN ID on the BMC and the MergePoint 5200 appliance are the same; otherwise, the BMC cannot communicate with the MergePoint appliance in the VLAN mode.

To set basic provisioning parameters in the MergePoint 5224/5240 appliance:

1. Click *Targets - Provisioning*.
2. In the Subnet drop-down menu, select a subnet.
3. Enter the username and gateway address in the fields provided.
4. In both the Password and Confirm Password field, enter the password.
5. Select *VLAN Enable* to use VLAN on the BMC, and specify the following parameters:
   a. In the VLAN ID field, type the VLAN ID.
   b. In the VLAN Priority field, type the VLAN priority.
6. Click *Apply*.

To set dynamic provisioning parameters:

1. Click *Targets - Provisioning*.
2. In the Dynamic Provisioning area, enter the Start and End IP addresses of a range of optional BMC IP addresses.
3. Click *Apply*.

To set static provisioning parameters:

1. Click *Targets - Provisioning*.
2. In the Static Provisioning area, click *Add* and specify the requested PXE parameters.
3. Click *Apply*.

NOTE: To modify the static IP address, click the name link and follow the on-screen instructions. To delete a static IP address, select the name link and click *Delete*.

BMC log

Once BMC provisioning starts, an activity log is displayed in the Provisioning window listing all IP addresses which have been assigned to target devices. A status of Confirmed or Unconfirmed is displayed for each target device in the specified IP address range. A status of Confirmed in the State column indicates that the BMC provisioning for that target device is complete and the target device can now be managed by the MergePoint SP manager.

To delete the provisioning log (Admin users only):

1. Click *Targets- Provisioning*.
2. In the Provisioning Log area, select the desired line(s) and click *Delete*.

Users

Managing MergePoint SP manager user accounts

The default user account username and password are both **admin**. Each MergePoint SP manager should have at least one Admin user. An Admin user account cannot be deleted if it is the only Admin user account configured.

You may specify a privilege of Admin, Operator, User or customized roles for each user account. The Admin privilege gives the user full control over all settings and the ability to perform any MergePoint SP manager operations, as well as manage all of the target devices in the MergePoint SP manager. The Operator privilege allows the user to perform basic operations, modify a limited number of settings and manage assigned target devices. A User privilege allows the user to view and query information of assigned target devices but prevents performing most operations and modifying most settings. Customized roles are created under the User Role tab. Customized role privilege is defined by users when they are created and provide the ability to access selected target devices and perform designated operations on those devices.

User accounts can also be managed in groups. After a user is added to a group, that user can manage all target devices assigned to it individually, as well as all the target devices assigned to any groups to which the user belongs.

To add an appliance user (Admin users only):

1. Click *Users - User Roles*.
2. Click *Add.*
3. Specify the following information for the new user:
   a. In the User Name field, type the username.

NOTE: Do not use reserved words for usernames. Reserved words that have special meaning for the MergePoint SP manager are listed in *Reserved Words* on page 145.

   b. In the Password field, type the password.
   c. From the Privilege drop-down menu, select the privileges you wish to assign to the user: *Admin*, *Operator*, *User* or customized roles.
   d. For Operator, User or customized role privilege users, select the target devices which can be managed by the user. For Admin privilege users, skip this step.
4. Click *Apply.*

To edit an appliance user (Admin users only):

1. Click *Users - Users.*

2. Click the username link for the user you wish to edit.
3. To change the password, select *Change Password*. Type the new password in the New Password and Confirm Password fields.
4. To change the privileges assigned to the user, select the desired privilege from the Privilege drop-down menu: Admin, Operator, User or customized roles.
5. For Operator, User or customized role privilege users, select the target devices which can be managed by the user. For Admin privilege users, skip this step.
6. Click *Apply.*

To delete an appliance user (Admin users only):

1. Click *Users - Users.*
2. Click the username link for the user you wish to delete and click *Delete*.

To customize a new role (Admin users only):

1. Click *Users - User Roles*.
2. Click *Add.*
3. In the Role Name field, type the name of the user role you want to create.
4. Check the operation(s) which you want this user role to access.
5. Click *Apply.*

To change the password for the user account (for Operator and User users only):

1. Click *Users - Users.*
2. Type the new password in the New Password and Confirm Password fields and click *Apply.*

To create a new user group (Admin users only):

1. Click *Users - Groups*.
2. Click *Add.*
   a. Specify the following information for the new user:
   b. In the User Group Name field, type the group name.
   c. In the Users area, select the users for the group.
   d. In the Targets area, select the target devices for the group.
3. Click *Apply.*

To edit a user group (Admin users only):

1. Click *Users - Groups*.
2. Click the link of the group name you want to edit.

To delete a user group (Admin users only):

1. Click *Users - Groups*.

2. Select the user group you want to delete and click *Delete*.

DHCP on the MergePoint SP Manager

The MergePoint SP manager has a Dynamic Host Configuration Protocol (DHCP) server to quickly and efficiently configure new devices on the Ethernet. It supports Dynamic and Static DHCP; static DHCP is performed before dynamic DHCP.

DHCP-assigned target devices can be added to a managed target device list automatically if the username and password of the device match the default username and password. Otherwise, the assigned target devices will be added into an unmanaged target device list.

DHCP on the MergePoint SP manager supports DHCP relay. The DHCP relay is a Bootstrap Protocol (BOOTP) relay agent that sends DHCP messages between DHCP clients and DHCP servers on different IP networks. After enabling DHCP relay, you must configure a DHCP relay server in another physical network.

Once DHCP starts, an activity log is displayed in the DHCP window listing all IP addresses which have been assigned to target devices.

To set the DHCP parameters in the MergePoint 5200 appliance:

1. Click *Targets - DHCP.*
2. For dynamic DHCP, specify the Start and End IP range of addresses in the dynamic DHCP area.
   -or-
   For static DHCP, click *Add* in the Static IP area and specify the requested parameters.
3. Click *Apply.*

To set the DHCP parameters in the MergePoint 5224/5240 appliance:

1. Click *Targets - DHCP.*
2. In the Subnet drop-down menu, select a subnet.
3. For dynamic DHCP, specify the Start and End IP range of addresses in the dynamic DHCP area.

   -or-

   For static DHCP, click *Add* in the Static IP area and specify the requested parameters.
4. Click *Apply.*

NOTE: To modify a static IP address, click on the name of the IP address and follow the on-screen instructions. To delete a static IP address, select the check box next to the name and click *Delete*.

To stop or start the DHCP service:

1. Click *Targets - DHCP.*

2. Click *Stop* or *Start* as appropriate.

To configure the DHCP relay server:

1. Click *Targets - DHCP.*
2. In the Status area, select *Enable* to activate DHCP relay.
3. In the Sever field, enter the IP address or the name of the DHCP relay server.
4. Click *Apply.*

NOTE: DHCP settings may also be changed using the CLI utility. See the related CLI commands on page 113.

Discovering and Adding Target Devices (Admin users only)

You can configure the MergePoint SP manager web interface to discover target devices that reside on the same LAN as the appliance by specifying one or more IP address ranges either for automatic or manual discovery. Discovered target devices are displayed in the Unmanaged Targets list, where you can select them for additions to the Managed Targets list. You can also manually add a target device if you know its IP address.

You may designate up to two IP address ranges for discovery. The first time you access the Targets window the IP address ranges are blank and may be modified by clicking *Edit*.

NOTE: For most of the target device types, you can view the target device types from the Type column in the Unmanaged Targets list. In a few cases, the target device types cannot be recognized until the target devices are managed and verified. For more details, see *Target Device Types Displayed in the Managed/Unmanaged Targets Lists* on page 28.

NOTE: Set RSA II devices to broadcast mode to avoid MergePoint SP manager discovery errors.

Discovering target devices

To discover target devices:

1. Click the *Targets* tab, then click *Targets* in the top navigation bar.
2. Select *Discovery Setting*, then click *Edit* next to the IP address range you wish to modify.
3. In the Subnet Edit window, define the range of IP addresses that will be searched during discovery.
4. Select either of the following start modes:

   For the MergePoint SP manager to automatically search for target devices in the specified IP address range at the specified time interval, select *Automatic*. If you wish to repeat the discovery sooner, click the *Start* link next to the IP address range.

NOTE: To set the time interval, see *To set discovery time interval:* on page 26.

- or -

If you want the MergePoint SP manager to search for target devices in the specified IP address range one time, select *Manual*.

5. Click *Apply.*

NOTE: Discovery results from either start mode will be displayed in the Unmanaged Targets list in the Targets window.

To set discovery time interval:

1. Click the *Targets* tab, then click *Targets* in the top navigation bar.
2. Select *Discovery Setting*.
3. In the Time Interval field, type the value of minutes for the time interval.
4. Click *Apply.*

NOTE: The time interval is only used for the automatic discovery. The value of the time interval may be between 5 and 65535 minutes. The preset value is 30 minutes.

Manually Adding a Single Target Device

If you already know the IP address of a target device, you may add it manually. In addition, you can require verification of a specified username and password when a user connects to the target device. The verified target devices and unverified target devices are distinguished using different icons in the explorer tree in the side navigation bar. An icon with a key indicates a verified target device.

Added target devices are displayed in the Managed Targets list. A green checkmark indicates a verified target device, while a red X indicates an unverified target device.

To manually add a target device:

1. Click the *Targets* tab, then click *Targets* in the top navigation bar. The Targets window appears.
2. Click *Manually Add Target*. The Input Target Information window appears.
3. In the IP field, type the service processor IP address of the new target device.
4. In the Alias field, type the alias for the new target device.
5. If you want to require a username and password when connecting to the target device, select *Verify username and password.*
   a. To use the preset credentials configured by the manufacturer, select *Use default username and password*.
      - or -
      To use a new username and password, select *Do not use default username and password* and enter the username and password in the corresponding fields.
   b. Select or deselect *Data Buffering* as desired. (To set SoL data buffering size, see *To set the session time interval and SoL history size:* on page 35*)*.

-or-

If you do not want to require a username and password when connecting to the target device, select *Don't verify username and password.* You may specify the username and password in the corresponding fields for accessing other functions.

NOTE: If *Verify username and password* is selected, the username and password are checked when adding a target device and the Serial over LAN (SoL) session starts automatically. If *Verify username and password* is deselected, the username and password are not checked when adding a target device and the SoL session is not started.

NOTE: From the SP Profile drop-down menu, select the SP profile of the new target device.

NOTE: There are two types of SP profiles: default SP profiles and user SP profiles. If you choose a user SP profile, then you have to define a type for it.

6. (Optional) From the Type drop-down menu, select the type of the new target device.

NOTE: The Type drop-down menu only appears when you select a user SP profile from the SP Profile drop-down menu. The selected type must match the selected SP profile.

7. (Optional) In the KG field, type the BMC key.

NOTE: The KG field only appears when you select *IPMI* from the SP Profile drop-down menu. A BMC key is required by IPMI 2.0 and RMCP+ (Remote Mail Checking Protocol).

8. (Optional) From the Group Name drop-down menu, select a group for the new target device. The target device will be listed in the group folder in the side navigation bar.
9. From the SoL access type drop-down menu, select the SoL access type for the new target device.

NOTE: The SoL access type drop-down menu only appears when you select *iLO* from the SP Profile drop-down menu.

10. Click *Apply.* Discovery results are displayed in the Managed Targets list in the Targets window.

Added target devices are displayed in the Managed Targets list. When adding a BladeCenter target device with a verified username and password, all blades are added at once. Otherwise, its blades are not added and are not available under the corresponding chassis in the main Unit Overview window. If you want to add blades now, you must change the verification status and then click the *Resync* button.

The settings of a target device can be modified on the Properties page of the target device. For more information, see *Changing target device parameters* on page 52.

NOTE: When a target device with a directcommnd-only SP profile is added to the MergePoint SP manager, a username and password is not required. In this case, you are not permitted to edit username and password related settings or require target device verification.

Managing Target Device Lists (Admin users only)

Discovered target devices are displayed in the Unmanaged Targets list, while manually added target devices are displayed in the Managed Targets list. You may add a target device to the Managed Targets list at any time. When you manage a target device, you can require verification of a specified username and password when a user connects to the target device.

If the managed target is part of a group or groups, it is displayed in the side navigation bar as part of the group folder(s).

NOTE: Users that do not have Administrator access will only see devices to which they have access.

For most of the target device types, you can view the target device types from the Type column in the Managed/Unmanaged Targets list. In a few cases, the target device types cannot be recognized until the target devices are managed and verified. See the following table for details.

Table 2.2: Target Device Types Displayed in the Managed/Unmanaged Targets Lists

Target Device Type	Display Type - Unmanaged	Display Type - Managed (Unverified)	Display Type – Managed (Verified)
IBM RSAII	IBM RSAII	IBM RSAII_withoutSol	IBM RSAII
IBM RSAII_withoutSol	IBM RSAII	IBM RSAII_withoutSol	IBM RSAII_withoutSol
DELL DRAC III	Dell DRAC	Dell DRAC IV	Dell DRAC III
DELL DRAC 4	Dell DRAC	Dell DRAC IV	Dell DRAC IV
DELL 10G	IPMI2.0	IPMI 2.0	Dell 10G
FSC iRMC	IPMI2.0	IPMI 2.0	FSC iRMC 2.0
HP IPMI	IPMI2.0	IPMI 2.0	IPMI(HP) 2.0
Sun ILOM	IPMI2.0	IPMI 2.0	Sun ILOM

To add a target device to the Managed Targets list:

1. Click the *Targets* tab, then click *Targets* in the top navigation bar. The Targets window appears.
2. In the Unmanaged Targets list, select the target device you wish to add and click *Manage*. The Input Target Information window appears.
3. If you want to require a username and password when connecting to the target device, select *Verify username and password.*
   a. To use the preset credentials configured by the manufacturer, select *Use default username and password*.
   - or -

To use a new username and password, select *Do not use default username and password* and enter the username and password in the corresponding fields.

b. Select or deselect *Data Buffering* as desired. (To set SoL data buffering size, see *To set the session time interval and SoL history size:* on page 35*)*.

-or-

If you do not want to require a username and password when connecting to the target device, select *Don't verify username and password.* You may specify the username and password in the corresponding fields for accessing other functions.

NOTE: If *Verify username and password* is selected, the username and password are checked when adding a target device and the Serial over LAN (SoL) session starts automatically. If *Verify username and password* is deselected, the username and password are not checked when adding a target device and the SoL session is not started.

---

4. (Optional) Select *Group Name*. From the Group Name drop-down menu, select a group for the new target device. The target device appears in the group folder in the side navigation bar.
5. Click *Apply.*

Added target devices are displayed in the Managed Targets list. When adding a BladeCenter target device with a verified username and password, all blades are added at once. Otherwise, its blades are not added and are not available under the corresponding chassis in the main Unit Overview window. If you want to add blades now, you must change the verification status and then click the *Resync* button.

NOTE: Target device settings can be modified on the Properties page. For more information, see *Changing target device parameters* on page 52.

To delete a target device from the Managed/Unmanaged Targets list:

1. Click the *Targets* tab, then click *Targets* in the top navigation bar. The Targets window appears.
2. In the appropriate targets list, select the target device you wish to delete and click *Delete*.

To remove a target device from the side navigation bar:

1. In the side navigation bar, click a target device name.
2. Click the *Properties* tab.
3. In the top navigation bar, click *Target*. A window displaying target device information appears.
4. Click *Remove*. When prompted, confirm the remove action. The selected target device is removed from the side navigation bar.

To add a target device to a group:

1. In the side navigation bar, click a target device name.
2. Click the *Properties* tab.
3. In the top navigation bar, click *Target*. A window displaying target device information appears.

4. To add the target device to a group, click *Copy To*. From the Group drop-down menu, select a group. The target device is added to the new group and remains in the current group.
   -or-
   To move the target device to a new group, click *Move To*. From the Group drop-down menu, select a group. The target device is added to the new group and removed from the current group.
5. Click *Apply.*

Managing Target Device Groups (Admin users only)

You may create groups for managed target devices so you can perform operations on all devices in a group at the same time. You may create an unlimited number of groups, and the same target device may be a part of multiple groups.

A default target device group with the same name as the MergePoint SP manager alias is automatically created for you. In the side navigation bar, the appliance, target devices and target devices group are displayed in the explorer tree according to hierarchy. Group folders and target devices that are part of the appliance alias group are displayed one level below the MergePoint SP manager. Target devices that are members of groups are displayed one level below the corresponding group folder.

To add a new target device group:

1. Click the *Targets* tab, then click *Groups* in the top navigation bar.
2. Click *Add*.
3. In the Group Name field, type a name for the group, then click *Apply.*

To modify a target device group name:

1. Click the *Targets* tab, then click *Groups* in the top navigation bar.
2. In the Group list, click the name link you wish to modify.

   - or -

   Click a group name from the explorer tree in the side navigation bar, click *Configuration* in the top navigation bar, then click *Modify Name*.
3. In the Group Name field, type a name for the group, then click *Apply.*

To delete a device group:

1. Click the *Targets* tab, then click *Groups* in the top navigation bar.
2. In the Group list, select the group you wish to delete, then click *Delete*.

   - or -

   Click a group name from the explorer tree in the side navigation bar, click *Configuration* in the top navigation bar, then click *Delete*.

To add a managed target device to a device group:

1. Click the *Targets* tab, then click *Targets* in the top navigation bar.
2. In the Managed Targets list, select the target device you wish to add to a group, then click *Add Targets to Group*.
3. From the Group Name drop-down menu, select the group to which you wish to add the target device, then click *Apply.*

To configure device group actions:

1. Click *System - Setting.*
2. Enter the number of target devices to power on simultaneously in a group.
3. Enter the time interval in seconds to elapse between power on each target device in a series of grouped target devices.
4. Enter the number of target devices to power off simultaneously in a group.
5. Enter a command delay to power off units in a series (seconds).
6. Click *Apply.*

Managing SP Profiles (Admin users only)

The MergePoint SP manager supports two types of SP profiles: default and user. Default SP profiles define 18 default types of target devices, while user SP profiles define new target device types. The Admin user can view the settings of the default SP profiles and create, modify or delete a user SP profile. You may need to create a new SP profile if a target device does not work properly with any of the default SP profiles.

The SP profile provides parameters, values or functions of target devices, such as:

- Protocol: used for communications between the MergePoint SP manager and target devices.
- Family: contains a list of pre-defined SP profiles and customX (X=1, 2, 3) SP profiles.

NOTE: The customX family needs a new Expect script which has been created using the name talk_customX.exp. (For more on creating new Expect scripts, see *Profile Configuration* on page 131.)

- Command Template: contains a list of templates for SP profiles. You may create a new template by clicking *SP Templates Configuration.* A MindTerm session will activate the sptemplate utility. See *To use the sptemplate utility to create a new template:* on page 135. The new template is added to lists of command templates and becomes available for using when configuring target devices. The following target device types do not need a template:
  - IPMI type devices.
  - Target devices being configured only for Native IP access.
  - Target devices being configured for DirectCommand only access.
- DirectCommand Options: contains values to be used when DirectCommand is launched. The DirectCommand feature allows transparent access to native TCP services on a target

device, such as a Virtual Media interface or a native KVM implementation. You may configure up to 20 TCP service ports to set up port forwarding for DirectCommand.

When adding a new target device, an Admin user should follow the procedure under *To find out if an existing command template works with a new target device:* on page 134 to see if one of the default command templates works with the new target device. If not, an Admin user can use the MergePoint SP manager to either modify an existing user SP profile or create a new one.

To configure a new SP profile:

1. Click *Targets - SP Profiles.*
2. In the User SP Profiles area, click *Add.*
3. In the SP Profile window, specify the name, protocol, family and SP template for the new SP profile.

NOTE: SP profile names may only contain letters and numbers. Special characters, such as a space or slash, are not permitted.

NOTE: The SP template for the profile must be the same template used for the family you chose. New SP templates that you create will appear here. For more information, see *To use the sptemplate utility to create a new template:* on page 135.

4. Configure the DirectCommand parameters for the accessing the web interface of the SP profile by selecting a web scheme of *http* or *https*, entering a web port and entering the web address.
5. Configure TCP parameters for accessing TCP service on the new SP profile:
   a. In the TCP Port field, type the TCP service port you want to access.
   b. In the Description field, type the description of the service you are configuring.
   c. In the Warning drop-down menu, select *Yes* or *No*.

NOTE: You may configure up to 20 TCP ports.

6. Click *Apply.* The new SP profile will be displayed in the User SP Profiles list.

To view the settings of the default SP profiles:

1. Click *Targets - SP Profiles.*
2. Select the desired SP profile in the Default SP Profiles area.

To delete user SP profiles:

1. Click *Targets - SP Profiles.*
2. In the User SP Profiles list, select the SP profile you wish to delete and click *Delete*.

To modify a user SP profile:

1. Click *Targets - SP Profiles.*
2. In the User SP Profiles list, click the name link for the SP profile you wish to modify and enter the new information.

3. Click *Apply.*

Managing Default Users (Admin users only)

To perform management operations through a MergePoint SP manager, a username and password are required to access the target device. To simplify the authentication process, you may configure a default username and password for specific target devices. When a management operation is requested, the MergePoint SP manager searches the entire list of default usernames to see if there is an appropriate one for accessing the target device. You may create multiple entries of the same username with a different password for each.

One default username and password for each type of target device is created by default.

- For IPMI target devices, the default username is **null** and the password is **null**.
- For DRAC 3, DRAC 4, DRAC 5, DRAC/MC and Dell 10G target devices, the default username is **root** and the password is **calvin**.
- For IBM BladeCenter or RSA II target devices, the default username is **USERID** and the password is **PASSW0RD**.
- For ALOM target devices, the default username is **admin** and the password is **admin**.
- For ILOM target devices, the default username is **root** and the password is **changeme**.

NOTE: This feature is not supported on target devices equipped with iLO.

NOTE: The maximum number of default target users is five.

To add a default user:

1. Click *Targets - Default Target User - Add*.
2. Specify the information for the default target device user and click *Apply.*

To delete a default user:

1. Click *Targets - Default Target User.*
2. Select the user you wish to delete and click *Delete.*

To edit a default user:

1. Click *Targets - Default Target User.*
2. Click the username you want to modify.

Managing user accounts on target devices

The Users window lists all user accounts for the selected target device. MergePoint SP manager users with Admin privileges may change user account information on target devices.

NOTE: This feature is available for target devices that have user management functions. Different types of devices have different user management systems. For example, while some may allow adding, editing and deleting user accounts, others may only allow editing user accounts.

To edit a user account:

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, click *Users*.
4. Click the name of the user you want to modify or the *Edit* link next to the user.
5. Enter the desired changes, then click *Apply.*

To create a new user account:

NOTE: Some target devices support limited users. In this case, you are not able to add a new line of user information. However, you may create a new user account by defining a username, password and user privilege to a user that does not have a username.

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, click *Users*.
4. Click *Add* or click *Edit* next to a user without a username.
5. Enter the desired changes, then click *Apply.*

To remove a user account:

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, click *Users*. The Users window appears.
4. Select the user to be deleted and click *Delete.*
   -or-
   Click *Remove User* next to the user you wish to remove.

NOTE: The line of the removed user will not disappear from the user list. Instead, it will become a user without a username that has Guest user privilege (no matter which user privilege it had before).

Configuring the MergePoint SP Manager System

System settings (Admin users only)

To change the MergePoint SP manager alias:

1. Click *System - Setting*.
2. In the Alias field, type the new name for the MergePoint SP manager and click *Apply.*

To set target BMC time (for IPMI target devices only):

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, select *Time*. The Set Time window appears.
4. To synchronize the BMC time with the appliance time clock, select *Sync with Appliance*.
   -or-
   To synchronize the BMC time with the console time clock, select *Sync with Client PC*.
   -or-
   To specify the BMC time, select *Other* and select the time from the pop-up calendar.
5. Click *Apply.*

To set the session time interval and SoL history size:

1. Click *System - Advanced Setting*.
2. Input the desired settings in the fields provided and click *Apply.*

To set the MergePoint appliance time:

1. Click *System - Advanced Setting*.
2. Select *Synchronize with Client PC* to synchronize the MergePoint appliance time with the client PC.

   - or -

   Select *Other* and specify the MergePoint appliance time from the pop-up calendar.
3. Click *Apply.*

To set the Internet time server:

1. Click *System - Advanced Setting*.
2. In the Internet time server field, enter the Internet time server address.
3. (Optional) Click *Update Now* to immediately synchronize the MergePoint appliance with the Internet time server.
4. (Optional) Select *Automatically synchronize with an Internet time server* to synchronize the MergePoint appliance with the Internet time server every 36 hours.
5. Click *Apply.*

To set MergePoint SP manager time zone:

1. Click *System - Advanced Setting*.
2. Select a time zone other than Custom from the Appliance Time Zone drop-down menu.
3. Click *Apply.*

NOTE: The Appliance Current Time field displays the current appliance time in the local time zone, based on the time zone location settings on your client PC. If you change the MergePoint appliance time zone, but do not change any other time settings such as the appliance time or client PC time zone, the Appliance Current Time is not affected and the value in the field does not change.

To configure the MergePoint SP manager for a customized time zone:

1. Click *System - Advanced Setting*.
2. Select *Custom* from the Appliance Time Zone drop-down menu.
3. Click *Edit Custom*.
4. In the Timezone name field, type the name of the time zone.
5. In the Standard Time Acronym field, type a standard acronym for the time zone.
6. In the GMT off drop-down menu, select the GMT offset.
7. (Optional) Select *Enable daylight saving time* if you would like to configure the MergePoint SP manager with DST.
    a. In the DST Acronym field, type the daylight saving time (DST) acronym of your choice.
    b. In the Saving time drop-down menu, select the number of hours and minutes in the HH:MM format. The clock will be reset at the beginning of the daylight saving time period.
    c. In the DST start fields, select the start dates of daylight saving time from the pop-up calendar.
    d. In the DST end fields, select the end dates of daylight saving time from the pop-up calendar.
8. Click *Apply.*

To enable or disable the Telnet or SSH protocol:

1. Click *System - Setting*.
2. Select or deselect *Telnet* or *SSH* to enable/disable the respective protocol.
3. Click *Apply.*

NOTE: (For the MergePoint 5224/5240 appliance ONLY) In some cases, such as soon after an upgrade, enabling the SSH protocol may be delayed while the service processor initiates.

PCMCIA for the MergePoint 5224/5240 Appliance

The front panel of the MergePoint 5224/5240 appliance has two PCMCIA card slots supporting compact Flash PC cards.

Two PC cards of the same type must be installed with the card in slot 1 configured first, followed by the card in slot 2. Two PCMCIA cards of different types can be installed in any order.

To install a PCMCIA card:

1. Insert a PCMCIA card into a front slot and slide the card in all the way.
2. Click *System - PCMCIA*.
3. Select the slot you inserted the card into and click *Insert*.

NOTE: Always use the Eject button in the MergePoint SP manager to eject the PCMCIA card.

To eject a PCMCIA card:

1. Click *System - PCMCIA*.
2. Select the slot for the card you are removing and click *Eject*. Then physically remove the card from the PCMCIA slot.

Completing the MergePoint SP Manager Installation

Whatever method is used to enable access to the web interface, the root user should always log into the MergePoint SP manager console and change the password from the default. The admin user cannot change the root user password, and the root user cannot log into the web interface to change the root password. The following options are available:

- Until an IP address is available for the MergePoint SP manager, the root user can only change the root user password by logging in locally through the console port.
- After an IP address is available for the MergePoint SP manager, the remote root user can use SSH to connect to the console and log in from a remote location and change the password.

CHAPTER 3

Operations

The operations in this chapter are performed using the MergePoint SP manager web interface. For instructions on using the MergePoint SP manager with DSView 3 software, please see the DSView 3 Software Installer/User Guide.

When the MergePoint SP manager is selected in the side navigation bar, a line of tabs and sub-tabs appears in the tab bar. They vary according to the user access level. For users without administrator access, only the Targets, Users and Alerts tabs are available.

- Targets: Used to display and manage discovered target devices.
- System: Used to define or change MergePoint SP manager settings.
- Network: Used to configure MergePoint SP manager network settings.
- Users: Used to manage MergePoint SP manager user accounts.
- Alerts: Used to view, query and activate system alerts.
- Accounting Log: Used to view all MergePoint SP manager operations.
- Diagnostic: Used to collect all network packets between a target device and a MergePoint SP manager for troubleshooting and problem resolution.

Using the MergePoint SP Manager

The operations described in this chapter are performed through the MergePoint SP manager web interface. For installations involving multiple MergePoint SP managers, the same functions can be accessed through the DSView 3 software. For information on using the DSView 3 software with the MergePoint SP manager, please see the DSView 3 software installer/user guide and the online help for the MergePoint SP manager plug-in.

MergePoint SP manager web interface

You can connect to the MergePoint SP manager web interface using any of the following web browsers or their later releases: Internet Explorer 6.0, Firefox 1.0 or Mozilla 1.4.

To access the MergePoint SP manager web interface:

1. Open a web browser and enter the IP address of the MergePoint SP manager.
2. Enter your username and password and click *Login*.

NOTE: When following any of the MergePoint SP manager configuration procedures in this document, start by clicking the name of the MergePoint SP manager in the side navigation bar. Click *Apply* to save changes. To cancel changes, click *Back* to return to the previous screen or click another navigation element, such as the name of a tab, window or target.

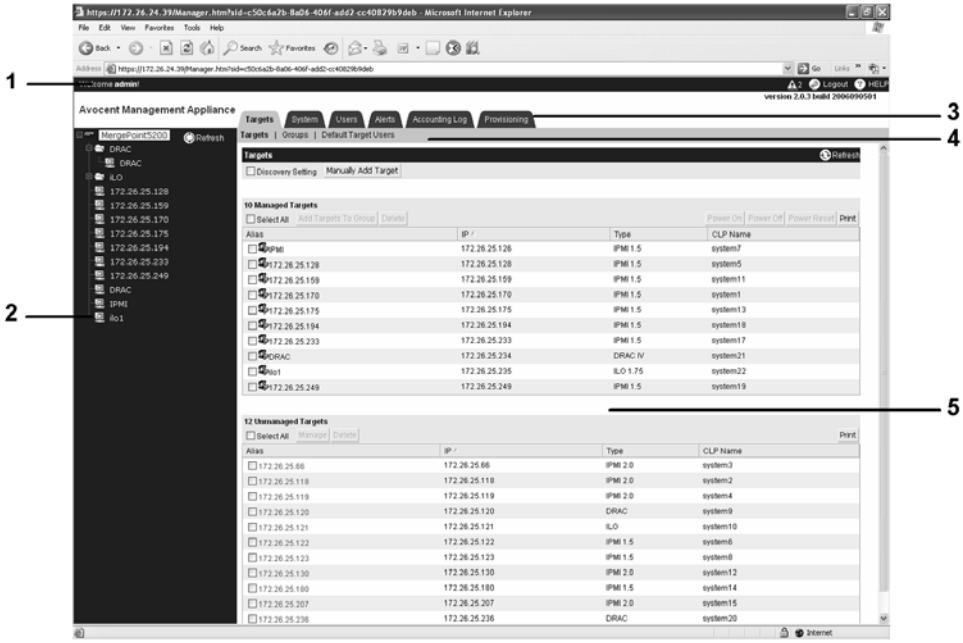


Figure 3.1: MergePoint 5200 Appliance Web Interface

Table 3.1: MergePoint 5200 Appliance Web Interface Descriptions

Number	Window Area	Description
1	Top Option Bar	Use the top option bar to log out or access online help. If any alerts occur, a yellow icon is displayed. The name of the logged in user appears on the left side of the top option bar.
2	Side Navigation Bar	Use the side navigation bar to select the appliance or target devices and access or edit corresponding information in the content area.
3	Tab Bar	Use the tab bar to display and manage the MergePoint SP manager, managed groups and target devices.
4	Top Navigation Bar	The selections in the top navigation bar vary, depending on the active tab in the tab bar.
5	Content Area	The content area displays information relative to your selections and allows you to make changes to the MergePoint SP manager, managed groups or target devices.

Power Management

Remote power and chassis management

Using the MergePoint SP manager, you may view the power status and the status of the chassis indicator LED (if available) on managed target devices, manage power and turn the LED on and off remotely. You may also initiate cold reset and self test operations on certain types of target devices.

The effects of Power Off and Power Cycle commands differ among service processor vendors. For a hard power command, power is turned off immediately, while a soft command shuts down the operating system before powering down. If a service processor provides more than one of the options, the MergePoint SP manager performs the hard power option by default.

The options for the reset command also differ, and are defined as warm reset and cold boot. For a warm reset, only the operating system is restarted while a cold boot issues a power cycle command. In cases where both options are available, the MergePoint SP manager will use cold boot.

NOTE: In addition, for Dell 10G target devices, you can view power tracking statistics and peak statistics by clicking *Power Monitoring*.

To view and control the power status:

1. In the side navigation bar, click a target device name.
2. Click the *System* tab.
3. In the top navigation bar, click *Power*. The Power Information window appears and displays the current power status of the target device.
4. Following the instructions on the page, select the desired power action: *Power On*, *Power Off*, *Graceful Shutdown*, *Power Reset*, *Power Cycle* and *Soft Reset*.

To monitor power for target device Dell 10G:

1. In the side navigation bar, click a target device name.
2. Click the *System* tab.
3. In the top navigation bar, click *Power Monitoring*.

NOTE: Make sure the correct SP profile is selected for the Dell 10G target device; otherwise, the Power Monitoring tab is not visible. To modify the target device SP profile, see *To change target device parameters:* on page 52.

To turn on, turn off or reset all selected target devices:

1. Click the *Targets* tab, then click *Targets* in the top navigation bar. The Targets window appears.
2. In the Managed Targets list, select the target device(s) you wish to manage and click the desired power operation.

To view and control the chassis status (LED):

1. In the side navigation bar, click a target device name.
2. Click the *System* tab.
3. In the top navigation bar, click *Chassis*. The Chassis Information window appears and the current chassis status of the target device is displayed.
4. To modify how often the LED flashes, enter the number of seconds in the Indicator ON Seconds field.
5. To change the chassis indicator status of the target device, complete any of the following steps:

   To turn the LED on and leave the LED flashing for a specified number of seconds, click *Indicator On Seconds*. The LED flashes for the time specified in the Indicator On seconds field.

   - or -

   To turn the LED on and leave the LED flashing permanently, click *Indictor On*.

   - or -

   To turn the LED off, click *Indicator Off*.
6. Click *Apply.*

To perform a cold reset on a target device:

1. In the side navigation bar, click a target device name.
2. Click the *System* tab.
3. In the top navigation bar, click *Advanced Tools*. The Setting window appears.
4. Click *Cold Reset* to perform a cold reset on the selected target device. A message will appear to indicate the success status of the cold reset.

To reboot the MergePoint SP manager:

Click *System – Setting - Apply Reboot*.

Performing Target Device Group Operations

Admin users may perform the following for all target devices in a group at the same time: turn on, turn off or reset the devices, turn the target device LED indicators on or off, and configure time, Platform Event Trap (PET) alert settings, usernames and passwords.

You can also move or copy target devices from one group to another, and remove target devices from a group.

NOTE: A group must contain at least one target device before you can perform a group operation.

To turn on, turn off or reset all target devices in a group:

1. Click *Targets - Group*.
2. Select the group(s) you wish to modify and click the desired power operation.

   - or -

   Click a group name from the explorer tree in the side navigation bar, click *Action* in the top navigation bar, then click the desired power operation.

To turn LED indicators on or off for all target devices in a group:

1. Click *Targets - Group*.
2. Select the group(s) you wish to modify and click the desired indicator state.

   - or -

   Click a group name from the explorer tree in the side navigation bar, click *Action* in the top navigation bar, then click the desired indicator state.

To set the time for all target devices in a group:

1. Click *Targets - Group*.
2. Select the group(s) you wish to modify and click *Set Time*.

   - or -

   Click a group name from the explorer tree in the side navigation bar, click *Action* in the top navigation bar, then click *Set Time*.

3. To synchronize the target devices with the MergePoint SP manager time clock, select *Synchronize with Appliance*.
   -or-
   To synchronize the target devices with the client PC time clock, select *Synchronize with Client PC*.
   -or-
   To specify the time, select *Other* and select the time from the pop-up calendar.
4. Click *Apply.*

To change the PET alert settings for all target devices in a group:

1. Click *Targets - Group*.
2. In the Group list, select the group(s) you wish to modify and click *PET Setting*.

   - or -

   Click a group name from the explorer tree in the side navigation bar, click *Action* in the top navigation bar, then click *PET Setting*.

3. Perform any of the following steps:

a. Enable or disable *Send Alerts*. Enabling this function allows the BMC to send alerts when events occur.
b. In the Community String field, type the value that will be displayed in the PET trap community string field.
c. Type up to four IP addresses in the Alert Destination IP Address fields.

NOTE: To allow the MergePoint SP manager to receive alerts from the target device, one field should contain the IP address of the MergePoint SP manager.

4. Click *Apply.*

To set a user and password for all target devices in a group:

1. Click *Targets - Group*.
2. In the Group list, select the group(s) you wish to modify and click *Set User and Password*.

   - or -

   Click a group name from the explorer tree in the side navigation bar, click *Action* in the top navigation bar, then click *Set User and Password*.
3. Enter the requested information and click *Apply.*

To manage target device groups:

1. Click a group name from the explorer tree in the side navigation bar.
2. Select the desired target device(s) you wish to copy/move to the group, or remove from the group.
3. Click the corresponding button and follow the on-screen instructions.

Monitoring and Management

Viewing sensor status

The MergePoint SP manager can detect the status of fan, temperature and voltage sensors on managed target devices. By clicking the *Sensor* tab, you may view a detailed report of a device's sensors that includes the sensor name, type, current reading and status.

NOTE: For some types of target devices, you can change a temperature scale to view sensor information.

To view sensor status:

1. In the side navigation bar, click a target device name.
2. Click the *Sensor* tab.
3. In the top navigation bar, click *Sensor.* The Sensor window and a detailed list of sensors and corresponding information appears.

Viewing SEL events

You may use the MergePoint SP manager to view the SEL (System Event Log) on a managed target device.

To view SEL events:

1. In the side navigation bar, click a target device name.
2. Click the *SEL* tab.
3. In the top navigation bar, click *SEL*. The SEL window and a detailed SEL event list appears.

To clear the SEL events:

1. In the side navigation bar, click a target device name.
2. Click the *SEL* tab.
3. In the top navigation bar, click *SEL*. The SEL window appears.
4. Click *Clear All SEL*. All currently listed events are removed from the list.

Viewing the accounting log

The accounting log records and displays all MergePoint SP manager operations. The WEB accounting log displays operations performed using the MergePoint SP manager web interface. Mgpshell accounting log displays operations performed using Mgpshell. Detailed information including operation time, login username, operation type, target device and console IP are displayed in the accounting log.

To view the accounting log (Admin users only):

1. Click the *Accounting Log* tab.
2. Click *WEB* to view operations performed through the MergePoint SP manager web interface.

   -or-

   Click *Mgpshell* to view operations performed through the Mgpshell.

Import/export data

This function allows you to backup and restore the MergePoint SP manager by exporting the data to the client PC or a storage location on the network.

NOTE: See the MergePoint SP manager release notes for more information about restoring data in MergePoint SP manager.

To export data from the MergePoint SP manager (Admin users only):

1. Click the *System - Import/Export.*
2. Click *Export.* All MergePoint SP manager data will be compiled and a download link will appear next to the Export button.

3. Click *download* to save the data file to the desired location.

To import data to the MergePoint SP manager (Admin users only):

1. Click *System - Import/Export*.
2. In the Filename field, type the path to the file you wish to import or click *Browse* to locate the file.
3. Click *Import* to restore the data in the file to the MergePoint SP manager.

Accessing FRU information

The MergePoint SP manager can find and display some Field Replaceable Unit (FRU) information for the selected target device, including chassis type, board language code and product name.

To retrieve FRU information:

1. In the side navigation bar, click a target device name.
2. Click the *Properties* tab.
3. In the top navigation bar, click *FRU Information*. A detailed FRU information report appears.

Using the Alerts Viewer

The MergePoint SP manager logs user-defined alerts that occur on managed target devices in the Alert Viewer window. You may configure the MergePoint SP manager to send a notification by email, MSN, SNMP Forward or Yahoo! message when specific alerts occur.

The Alerts Viewer window displays alerts and the corresponding date/time, source, IP address, event type and severity level. Alerts set as read will be listed in black; alerts not set as read will be listed in red. Click *Detail* next to an alert to view additional information.

To locate specific alerts, you may specify parameters to query the list of alerts. Users can also search alert messages through a query analyzer. The query parameters include occurrence period, IP address, event type, severity level and read status.

Setting an alert action

You may create an alert action by configuring action parameters to your specifications. You may also configure the MergePoint SP manager to send email, MSN messages or Yahoo! messages to specific users, or forward SNMP messages to specific target devices once an alert occurs.

Before creating an alert action, configure the action settings to allow for alert notifications.

To configure action settings (Admin users only):

1. Click the *Alerts* tab.
2. In the top navigation bar, click *Action*.
3. Click *Action Setting*.
4. Specify the following parameters:

a. In the SMTP Server field, type the Simple Mail Transfer Protocol (SMTP) server address for sending email.
b. In the SMTP Server Account field, type the account used as the email sender.
c. In the SMTP Server Password field, type the password for the SMTP server account.
d. In the SMTP Sender field, type the display name of the email sender.
e. In the MSN User field, type the MSN account used as the MSN message sender.
f. In the MSN Password field, type the password for the MSN user.
g. In the YAHOO IM User field, type the YAHOO IM account used as the YAHOO IM message sender.
h. In the YAHOO IM Password field, type the password for the YAHOO IM account.

5. Click *Apply.*

To create an alert action (Admin users only):

1. Click the *Alerts* tab.
2. In the top navigation bar, click *Action.*
3. Click *Add.*
4. In the Action Configuration area, specify the following information:
   a. Select the Action Type from the drop-down menu: *Email, MSN, YAHOO or SNMP Forward.*
   b. If you selected *Email*, type the email address of the receiver in the Email Address field.
      -or-
      If you selected *MSN*, type the MSN account of the receiver in the Email Address field.
      -or-
      If you selected *SNMP Forward*, type the IP address of the destination machine in the Receiver field.
      -or-
      If you selected *YAHOO*, type the YAHOO IM account of the receiver in the YAHOO field.
5. Click *Apply.*

To delete an alert action (Admin users only):

1. Click the *Alerts - Action*.
2. From the list, select the action(s) you wish to delete and click *Delete*.

To query an alert (for all users):

1. Click the *Alerts* tab.
2. In the Alert Viewer area, select *Show Alert Query.*
3. In the Alert Query area, specify any or all of the following parameters for the query:
   a. Select *Period From* to enable date range fields.

b. In the Period From and To fields, type the date range for the alerts you wish to be included in the query results. The default value of the To field is the current date.

c. From the IP address drop-down menu, select either *All* or a specific IP address for the target devices you wish to be included in the query results.

d. From the Severity drop-down menu, select the severity of the alerts you wish to be included in the query results: *All, Specified, Monitor, Information, OK, NonCritical, Critical* or *Non-Recoverable.*

e. From the Read Status drop-down menu, select the read status of the alerts you wish to be included in the query results: *All, Read* or *Unread*.

4. Click *Query* to search the alerts. The qualifying alerts will be displayed in a list below the Alert Query area.

To set an alert as read (Admin users only):

1. Click the *Alerts* tab.
2. From the list, select the unread alerts you wish to modify.
3. Click *Set Selected Read* to mark the selected alerts as read. The alerts change from red to black text to indicate the read status.

To delete an alert (Admin users only):

1. Click the *Alerts* tab.
2. From the list, select the alerts you wish to delete.
3. Click *Delete Selected* to remove the alerts from the Alerts Viewer list.

Syslog

The Admin user can set up logging of messages about the following types of events:

- Events of interest from the MergePoint SP manager
- Events of interest obtained by filtering data during device console connections with connected devices
- Sensor alarms generated by sensors on target devices

Messages can be sent to a user defined destination. Messages can also be sent to the console, the root user or both.

Message filtering levels

Messages can be filtered according to their severity, based on any or all of the levels from the following list.

- 0 - Emergency
- 1 - Alert
- 2 - Critical

- 3 - Error
- 4 - Warning
- 5 - Notice
- 6 - Info
- 7 - Debug

Configuring syslog messages

To configure syslog message filtering:

1. Click *System - Syslog*.
2. Select the link of the filter name which you want to modify.
3. Click the checkboxes next to the desired severity levels.
4. Click *Apply* to finish.

To configure the syslog destination:

1. Click *System - Syslog*.
2. In the System Destination area, select *Console* to send messages to the console.
   -and/or-
   Click *Root user* to send messages to the root user.
3. In the User Define Destination area, configure messages to be sent to a defined syslog server as follows.
   a. Click *Add*.
   b. In the Syslog Destination field, type a syslog server's IP address.
   c. Click *Apply*.
   d. To add additional syslog servers, repeat steps a through c.

NOTE: You can edit or delete syslog servers by selecting the corresponding destination and clicking *Delete*.

Configuring PET alerts

Users with Admin privileges may configure PET alerts separately for each target device.

To configure PET alerts:

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, click *Event Destination*. The PET Setting window appears.
4. Select *Enable* or *Disable* for sending or not sending alerts when specific events occur.
5. In the Community String field, enter the value to be displayed in the community string field of the PET trap.
6. Enter up to four IP addresses in the Alert Destination IP Address fields.

7. Click *Apply.*

NOTE: To configure the MergePoint SP manager to receive alerts for the target device, make sure to enter the IP address of the MergePoint SP manager in one of the Alert Destination IP Address fields.

Schedules

Tasks can be scheduled to simultaneously turn on or off or reset the power on all target devices in a group. The results of each scheduled task display in the Schedule Task Result list in the Schedule Task window. To clear this list, click *Clear All*.

Schedule a task (Admin users only)

To schedule a task:

1. Click *System - Schedules*.
2. Click *Add* and select *Group* to display all device groups or *Targets* to display all target devices.
3. Specify the following information:
   a. Select the group(s) or target(s) for which you wish to schedule tasks.
   b. Type the task name into the Task Name field.
   c. From the Operate drop-down menu, select: *Power On*, *Power Off* or *Power Reset*.
   d. From the Schedule Task drop-down menu, select: *Once*, *Daily*, *Weekly* or *Monthly*.
   e. From the Time menu(s), select the day, hour and minute for the task to occur. Options in the Time menus vary according to your selections.
   f. Choose *Once*, *Daily*, *Weekly* or *Monthly*, then specify the task schedule accordingly.
4. Click *Apply.*

To edit a scheduled task:

1. Click *System - Schedules*.
2. Click *Edit* next to the task you wish to edit and follow the on-screen instructions.

To delete a scheduled task:

1. Click *System - Schedules*.
2. Select the task to delete and click *Delete*.

Target Operations

NOTE: As noted throughout this section, the available features vary according to the types of service processors. For example, accessing system information is only available for IPMI, ILOM, HP IPMI, FSC iRMC and Dell DRAC 5 devices; for other target devices, this feature cannot be viewed or accessed.

To perform any of these operations, access the MergePoint SP manager web interface. In the side navigation bar, click the name of the target device you wish to manage.

The following tabs are available:

- Properties: Use this tab to access system information and FRU, change the alias and copy or move the target device to a group. For a blade chassis that is managed as a target device, you can synchronize the blades with the target device.
- System: Use this tab to remotely perform system operations, including power, chassis and other advanced operations.
- Configuration: Use this tab to remotely configure managed target devices, including changing LAN parameters, managing user accounts, configuring PET settings, configuring SoL, setting BMC time, performing provisioning recovery and setting up SNMP and Native IP.
- SEL: Use this tab to view target device SEL information.
- Sensor: Use this tab to view the sensor output from managed target.
- Console: Use this tab to activate and use SoL for accessing managed target devices, the service processor console, Telnet console or SSH console.
- DirectCommand: Use this tab to transparently access native TCP services on a target device.
- Remote Control: Use this tab to connect to Remote Desktop Protocol (RDP) and Virtual Network Computing (VNC) servers.

Viewing target device information

To view the target device information:

1. In the side navigation bar, click a target device name.
2. Click the *Properties* tab.
3. In the top navigation bar, click *Target*. A window displaying target device information appears.

Synchronizing blades for a blade chassis

NOTE: The following procedure is only for target devices with blade chassis.

To synchronize the blades:

1. In the side navigation bar, click a target device name.
2. Click the *Properties* tab.
3. In the top navigation bar, click *Target*.
4. Click *Synchronize BladeCenter*. The blades on the side navigation bar are synchronized with the selected target device.

Changing the SoL port number

To change the SoL port number:

1. In the side navigation bar, click a target device name.
2. Click the *Properties* tab.

3. In the top navigation bar, click *Target*.
4. In the SoL Port field, type a SoL port number and click *Apply*.

Changing the access account of a target device

To change the access account of a target device:

1. Click the *Targets* tab. The Targets window appears.
2. In the Managed Targets list, click the desired target device link.
3. In the Username and Password field, type the username and password you would like to use to access the target device.
4. Click *Apply*.

NOTE: For an unverified target device, you can select *Verify the username and password* to verify the target device with the username and password you enter.

Changing target device parameters

You can modify target device parameters, including username and password, verification status, SP profiles and SoL access.

To change target device parameters:

1. In the side navigation bar, click a target device name.
2. Click the *Properties* tab.
3. In the top navigation bar, click *Target*. A window displaying target device information appears.
4. Click *Edit*. The Edit Target window appears.
5. In the Alias field, type the new name for the target device.
6. For an unverified target device, if you want to require a username and password when connecting to the target device, select *Verify username and password.*
   a. To use the preset credentials configured by the manufacturer, deselect *Change username and password*.
      - or -
      To use a new username and password, select *Change username and password* and enter the username and password in the corresponding fields.
   b. Select or deselect *Data Buffering* as desired. (To set SoL data buffering size, see *To set the session time interval and SoL history size:* on page 35*)*.

NOTE: If *Verify username and password* is selected, the username and password are checked when adding a target device and the Serial over LAN (SoL) session starts automatically. If *Verify username and password* is deselected, the username and password are not checked when adding a target device and the SoL session is not started.

For a verified target device, you may change the username and password in the corresponding fields for accessing other functions.

7. From the SP Profile drop-down menu, select the SP profile of the new target device.

NOTE: For more information on configuring SP profiles, see *Managing SP Profiles (Admin users only)* on page 31 and *Profile Configuration* on page 131.

8. From the SoL access type drop-down menu, select the SoL access type for the new iLO target device.

NOTE: This field only appears when you select *iLO* from the SP Profile drop-down menu.

9. Click *Apply*.

NOTE: For a target device with directcommnd-only SP profile, a username and password is not required. In this case, the username and password fields and target device verification fields are not shown.

To self test a target device:

1. In the side navigation bar, click a target device name.
2. Click the *System* tab.
3. In the top navigation bar, click *Advanced Tools*. The Setting window appears.
4. Click *Self Test* to perform a self test on the selected target device. A message will appear to indicate the success status of the self test.

Accessing system information

The MergePoint SP manager can find and display certain system information for the selected target device, including device ID, firmware version, IPMI version and manufacturer ID.

To retrieve system information:

1. In the side navigation bar, click a target device name.
2. Click the *Properties* tab.
3. In the top navigation bar, click *Information*. A detailed system information report appears.

Recovering provisioning

You can recover the original provisioning based on the configuration already in place at the target device.

To recover provisioning for a device:

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, click *Recover*. The Provisioning Recover window appears.
4. Click *Provisioning Recover*.

NOTE: The Provisioning Recover button is only available after the provisioning on this target device is performed successfully and confirmed.

Changing LAN parameters

To change LAN parameters:

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, click *LAN*. The LAN window appears.
4. From the IP Address Source drop-down menu, select *Static* or *DHCP* as the source type. If you select *Static* as the source type, specify the target device's IP address, subnet mask and gateway IP address in the fields provided.

NOTE: If you select DHCP, the target device's IP address is dynamically distributed from a DHCP server and the fields for configuring a static IP cannot be edited.

5. Click *Apply*.

SNMP

The SNMP agent provides access to the MergePoint SP manager through an SNMP management application, such as HP Openview, Novell NMS, IBM NetView or Sun Net Manager and provides proxy access to SNMP data from connected service processors that implement SNMP agents. The SNMP agent can be configured to send notifications (also known as traps) about significant events on the MergePoint SP manager and on target devices.

The administrator must configure the SNMP agent to use the version of SNMP supported by the management application, SNMP v1, v2c or v3. The use of v3 is strongly encouraged wherever possible because it provides authentication and encryption of data that is lacking in v1 and v2c.

Access to information provided by the MergePoint SP manager and its proxy target devices can be obtained in either of the two following ways:

- The recommended access method for agents which support only SNMP version 1 or 2c is through a proxy on the MergePoint SP manager. The MergePoint SP manager provides the authentication and encryption lacking in those protocol versions. The SNMP management application can then be used to for SNMP management of the target device.

NOTE: Running the SNMP daemon (snmpd) on the MergePoint SP manager allows you to access the proxy data using the v1 and 2c protocols without going through a VPN tunnel. However, this method is inherently unsecure.

- The access method agent which supports version 3 is via a local Net-SNMP daemon. The proxying of traps is not supported by Net-SNMP. Forwarding of traps is supported, with filtering by source address.

If SNMP is used as recommended, no public client is allowed unauthenticated access to either managed clients or to the MergePoint SP manager. For compatibility with other clients, unencrypted transfer of data is possible with SNMP v3 connections, but strongly discouraged.

- User and group information for v3 connections must be different from the user and group names used for accessing the MergePoint SP manager.

The administrator can configure the following:

- General information provided by the MergePoint SP manager, including location and contact fields
- Who has access to SNMP information
- Trap forwarding

Configuring SNMP

The Admin user can configure SNMP access for the MergePoint SP manager and for target devices. Admin users can enable alerts about significant events occurring on target devices to be sent from the MergePoint SP manager to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView or Sun Net Manager.

To configure appliance SNMP information:

1. Click *Network - SNMP.*
2. In the SysContact field, type the contact information of the MergePoint SP manager administrator.
3. In the SysLocation field, type the location of the MergePoint SP manager.
4. Click *Apply.*

To configure service processor SNMP settings:

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, click *SNMP.* The SNMP window appears.
4. In the OID field, type the identifier for the object to be managed.
5. From the SNMP version drop-down menu, select *v1*, *v2c* or *v3*.
6. If you selected either *v1* or *v2c*, type a community name in the Community field.
   -or-
   If you selected *v3*, enter the username required for authentication, the authentication method, the authentication password, the encryption method and, optionally, the encryption password in the fields provided.
7. Click *Apply.*

To configure users' SNMP access settings:

Perform this procedure to configure how users on the public side authenticate themselves to the MergePoint SP manager, whether they are using SNMP functionality on the MergePoint SP manager itself or SNMP functionality proxied from the device.

1. Click *Network - SNMP.*

2. In the Access settings area, click *Add*.
3. From the SNMP version drop-down menu, select a version.
4. If either the v1 or v2c version is selected in step 3, perform the following steps:
   a. In the Community field, type a community name.
   b. Select either *Default* or *Use IP* for the source.
   c. If Use IP is selected, type a source IP address.
   d. If a view has been configured, select a Read view and Write view from the drop-down menus. If no view has been configured, see *To configure views with SNMP v3:* on page 57.

   -or-

   If the v3 version is selected in step 3, perform the following steps:

   a. Select a user from User drop-down menu. See *To configure users with SNMP v3:* on page 56 for more information.
   b. For No Auth Security level, select a read view and write view under the Read view and Write view columns.
   c. For Auth Security level, select a read view and write view under the Read view and Write view columns.
   d. For Auth & crypt Security level, select a read view and write view under the Read view and Write view columns.
5. Click *Apply.*

NOTE: You may edit or delete an existing access setting by clicking the *Community/User* link and then following the on-screen instructions.

To configure users with SNMP v3:

If the v3 version is selected in step 3 of the previous procedure, configure users as desired by clicking *Add*. The User configuration dialog appears.

1. Click *Network - SNMP.*
2. In the Users area, click *Add*, then type a username.
3. Select an authentication method from the Auth method drop-down menu, then enter an optional authentication password.
4. Select an encryption method from the Encryption drop-down menu, then enter an optional encryption password.
5. Click *Apply.*

NOTE: You may edit or delete an existing user by clicking the username link and following the on-screen instructions.

To configure views with SNMP v3:

1. Click *Network - SNMP.*
2. In the View area, click *Add*, then enter a name for the view.
3. Select *Include* or *Exclude* from the drop-down menu to include or exclude the defined OIDsubtree.
4. Enter an OID for the object to be viewed and enter a mask to create an OID subtree in the fields provided. Repeat to create more OID subtrees as desired.
5. Click *Apply.*

NOTE: You may edit or delete an existing view by clicking the view name link and following the on-screen instructions.

Accessing a service processor's SNMP through the MergePoint SP manager

You can use third party utilities, such as "snmpwalk," to access a service processor's SNMP through the MergePoint SP manager. When using third party utilities, remember to add the context parameter (the service processor alias).

For example, you want to use the snmpwalk utility to access the SNMP of a MergePoint SP manager with an IP address of 172.26.25.99 and a community string of public158. The service processor alias is 172.26.25.158. To retrieve all SNMP information, enter the following command:

```
snmpwalk -v 1 -c public158 -n 172.26.25.158 172.26.25.99 .1.3.
```

The -n parameter is required prior to the service processor alias to specify which service processor you want to access.

NOTE: Visit www.net-snmp.org for more information about the snmpwalk utility.

Host table

The host table is a simple text file that allows Admin user to associate IP addresses with hostnames and alias.

To change the host name of the MergePoint appliance:

1. Select *Network - Host Table.*
2. Enter a host name for the MergePoint appliance in the Name field.
3. Click *Apply.*

To add an entry:

1. Select *Network - Host Table*, then click *Add*.
2. Enter the required information in the fields provided, then click *Apply.*

To edit an entry:

1. Select *Network - Host Table.*
2. Click the IP address link of the entry you would like to edit and follow the on-screen instructions.

To delete an entry:

1. Select *Network - Host Table.*
2. Select the entry(s) you would like to delete and click *Delete.*

Static routes

Admin users can use the Static routes feature to manually add, edit or delete existing static routes.

To add a static route:

1. Click *Network - Static Routes.*
2. Click *Add.*
3. In the Network Address field, type a network IP address of the destination host or specify a network in the form networkIPaddress/mask_length (also referred to as prefix/length).
4. From the Type drop-down menu, select Interface or Gateway as you desire.
5. If you select Interface, then choose an interface from the Interface/Gateway drop-down menu.
   -or-
   If you select Gateway, then in the Interface/Gateway field, type the IP of the gateway.
6. In the Metric field, type the number of hops to the destination.
7. Click *Apply.*

NOTE: To set a default route, select *Network - Network Settings*.

To edit a static route:

1. Click *Network - Static Routes.*
2. Click the network address link of the static route you want to edit and follow the on-screen instructions.

To delete a static route:

1. Click *Network - Static Routes.*
2. Click the network address link of the static route you want to delete and click *Delete*.

Using Serial over Lan (SOL)

Device console and service processor console

You may access four types of consoles on a target device: the device console, the service processor console, the Telnet console and SSH console.

Device console

You may access the device console via an SoL connection. SoL provides a mechanism that enables the serial controller of a managed device to be redirected via a service processor session over IP. This enables remote console applications to provide access to text-based interfaces for BIOS, utilities, operating systems and management services while simultaneously providing access to service processor functions.

NOTE: Before using the MergePoint SP manager SoL features, install the Java Runtime Environment (JRE) version 1.5 or later.

NOTE: A maximum of four simultaneous sessions are allowed from the DRAC/MC Web-based remote access interface. For DRAC/MC target devices, only one SoL connection to one blade is allowed at a time.

NOTE: For HP BladeCenter target devices, firmware version v1.3 or later is required for SoL.

To activate SoL:

1. In the side navigation bar, click a target device name.
2. Click the *Console* tab.
3. In the top navigation bar, click *Device Console*.The Device Console window opens.
4. Click *SoL* to activate the SoL window through a MindTerm client.

If the target device is a Windows server, an EMS/SAC prompt is returned. If the target device is a Linux server, the Linux serial console prompt is returned. Type valid SAC commands or Linux console commands in the MindTerm client to conduct SoL operations, such as BIOS configuration and power reset.

MindTerm is a third party client that supports a variety of terminal emulation programs. Not all terminal emulation programs support function keys or special characters, so certain keystroke sequences may be required for some commands. For example, in some applications, the function key F1 may be performed by entering **<ESC>1** on the keyboard. For more information, see the user guide for your terminal emulation program.

Enter **<Ctrl> + <[mouse right-click]>** for the MindTerm menu. From the menu, you can configure terminal settings, define tunnels and modify other settings. For example, to change the terminal emulation program, select *Settings - Terminal - Terminal Type*.

To view SoL history:

1. In the side navigation bar, click a target device name.
2. Click the *Console* tab.
3. In the top navigation bar, click *Device Console*. The Device Console window opens.
4. Click *SoL History* to display all the commands entered in SoL mode and their output.

NOTE: Dell DRAC/MC target devices do not support SoL history.

To replay SoL:

1. In the side navigation bar, click a target device name.
2. Click the *Console* tab.
3. In the top navigation bar, click *Device Console*. The Device Console window opens.
4. Click *SoL Replay* to replay SoL actions and results, including the BIOS result. Click and drag the speed bar to control replay speed.

Service processor console

You can also access the service processor console of the selected target device. After accessing the service processor console, you launch the management application from the service processor's command line.

To access service processor console:

1. In the side navigation bar, click a target device name.
2. Click the *Console* tab.
3. In the top navigation bar, click *SP Console*.The SP Console window opens.
4. Click *Connect*.

NOTE: After connecting to the service processor console, you can run any corresponding service processor console commands.

Telnet console

You can also access the Telnet console of the selected target device. After accessing the Telnet console, you can launch the management application from the service processor's command line.

To access the Telnet console:

1. In the side navigation bar, click a target device name.
2. Click the *Console* tab.
3. In the top navigation bar, click *Telnet Console*.The Telnet Console window opens.
4. Click *Connect*.

SSH console

You can also access the SSH console of the selected target device. After accessing the SSH console, you can launch the management application from the service processor's command line.

To access the SSH console:

1. In the side navigation bar, click a target device name.
2. Click the *Console* tab.
3. In the top navigation bar, click *SSH Console*.The SSH Console window opens.
4. Click *Connect*.

Configuring SoL parameters

The MergePoint SP manager allows you to define SoL parameters for target devices, including Enable/Disable Serial over LAN, baud rate and channel privilege limit level.

To configure SoL parameters:

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, click *Serial over LAN*. The Serial over LAN Configuration window appears.
4. Specify any of the following information:
   a. Select or deselect *Enable Serial over LAN* as desired.
   b. From the Baud Rate drop-down menu, select the baud rate.
   c. From the Channel Privilege Level Limit drop-down menu, select *Administrator*, *Operator* or *User* as the privilege level.
   d. From the Retry Count drop-down menu, select the number of times for a retry to occur, from *0* to *7* times.
   e. In the Retry Interval field, enter the number of 10 milliseconds to elapse between each retry.
5. Click *Apply.*

NFS

Network File System (NFS) provides remote access to SoL history information across networks. By default, SoL history information is saved to the MergePoint SP manager. To free memory space on the MergePoint SP manager, you may configure the SoL history data to be saved to another network location and access the SoL directories from anywhere on the network.

To configure NFS storage of SoL history data (Admin users only):

1. Click *System - NFS*.
2. Select *Enable* and specify the following information:
   a. In the Server IP field, type the IP address of the NFS server.
   b. In the Mount Directory field, type the directory pathname exported from the NFS server.
   c. From the Protocol drop-down menu, select the mount protocol.
3. Click *Apply.*

Remote control

You may connect to a Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC) server remotely through the MergePoint SP manager.

To connect to an RDP server:

1. In the side navigation bar, click a target device name.
2. Click the *Remote Control* tab.
3. In the top navigation bar, click *RDP*. The RDP window appears.
4. In the Server field, type the host operating system IP address (or hostname).
5. Click *Connect*.

To connect to a VNC server:

1. In the side navigation bar, click a target device name.
2. Click the *Remote Control* tab.
3. In the top navigation bar, click *VNC*. The VNC window appears.
4. In the Server field, type the host operating system IP address (or hostname).
5. In the Port field, type the port of VNC server.
6. Click *Connect*.

Diagnostics

The Diagnostics tab provides network trace and debugging tools by collecting all IP packets from an exchange between a network interface of the MergePoint SP manager and a target device. Traced information is saved to a trace file that can be downloaded. If needed, the downloaded trace file can be sent to Avocent technical support for troubleshooting assistance.

This trace and debug tool is implemented by tcpdump (see http://www.tcpdump.org/ for more information). First set up the data collection parameters before starting the tracing process. When the debug stops, click the *Download* button to create a download link.

To start the network debug:

1. Click the *Diagnostic* tab.
2. In the top navigation bar, click *Debug*.
3. Configure the interface, protocol, source IP, source port destination IP and destination port filtering options as needed.
4. Click *Start*.

NOTE: You must stop the debug manually; otherwise the debug process continues indefinitely. When the trace file size reaches to the maximum size (preset maximum is 1M), the trace file will be rewritten.

To stop the network debug:

1. Click the *Diagnostic* tab.
2. In the top navigation bar, click *Debug*.
3. Click *Stop*. Once stopped, you may download the trace file.

To download the trace file:

1. Click the *Diagnostic* tab.
2. In the top navigation bar, click *Debug*.
3. Click *Download*. All trace data is compiled and a download link appears next to the Download button.
4. Click the *Download* link to save the trace file.

NOTE: The trace file is stored on the server until the next debug starts.

NOTE: Diagnostics may also be configured using the CLI utility. See *Diagnostics CLI command -tcpdump* on page 119.

DirectCommand

DirectCommand allows transparent access to the MergePoint SP manager's web interface, vKVM interface or vMedia interface. The DirectCommand auto login feature provides a configurable option to log in automatically to the remote SP management web interface without needing to enter a username or password. The vKVM interface (or vMedia interface) allows you to enter the device KVM interface (or Media interface).

NOTE: DirectCommand requires Java SE Runtime Environment version 1.5.0_06. The Java SE Runtime Environment is available at www.sun.com.

To connect DirectCommand:

1. In the side navigation bar, click a target device name.
2. Click the *DirectCommand* tab.
3. Click *Connect*. Links will appear below the button. From these links you can go to the Browser Session interface, Browser Session (Auto Login) interface, vKVM interface or vMedia interface. A DirectCommand Connected link appears on the top option bar on the upper-right side of the page, where you can access the DirectCommand connection list window.

NOTE: The number of links depends on the type of target device. For example, only iLO has the vMedia interface. Most devices support the Browser Session (Auto Login) interface and the vKVM interface.

CAUTION: For proper operation, the vKVM port for RSAII device should be 2000.

DirectCommand connection list

When you select a target device and connect DirectCommand successfully, a DirectCommand Connected link appears on the top option bar on the upper-right side of the page. Clicking this link invokes the DirectCommand connection list showing all currently active connections. From this window you can access Browser Session interface, Browser Session Auto Login interface, vKVM interface or vMedia interface by clicking the corresponding button. You may also view the device connection information and forwarded ports from this window.

NOTE: The forwarded port information is retrieved from the TCP ports table in the SP profile. See *DirectCommand Options* on page 31.

To open the DirectCommand connection list window:

1. In the side navigation bar, click a target device name.
2. Click the *DirectCommand* tab.
3. Click *Connect*.
4. From the Top Option bar, click *Connected*. The DirectCommand connection list window appears.
5. You may view all of the currently active DirectCommand connections with their target device IP addresses here.

To enter the Browser Session interface:

1. In the side navigation bar, click a target device name.
2. Click the *DirectCommand* tab.
3. Click *Connect*, then click *Browser Session*.

   -or-

   From the Top Option bar, click *Connected*. The DirectCommand connection list window appears. Select the alias of the desired target device from the window, then click *DirectCommand*.

To enter the Browser Session (Auto Login) interface:

1. In the side navigation bar, click a target device name.
2. Click the *DirectCommand* tab.
3. Click *Connect*, then click *Browser Session* (Auto Login).

   -or-

   From the Top Option bar, click *Connected*. Select the alias of the desired target device, then click *Browser Session*.

To enter the vKVM Session interface:

1. In the side navigation bar, click a target device name.
2. Click the *DirectCommand* tab.
3. Click *Connect*, then click the *vKVM Session* link.

   -or-

   From the Top Option bar, click *Connected*. Select the alias of the desired target device, then click v*KVM Session*.

NOTE: Close any other open network applications, such as VNC, to avoid a port number conflict.

To enter the vMedia Session interface:

1. In the side navigation bar, click a target device name.
2. Click the *DirectCommand* tab.
3. Click *Connect*.
4. Click *vMedia Session*.

   -or-

   a. In the Top Option bar, click *Connected*.
   b. Select the alias of the desired target device, then click *vMedia Session*.

To disconnect DirectCommand:

1. In the side navigation bar, click a target device name.
2. Click the *DirectCommand* tab.
3. Click *Disconnect*.

   -or-

   a. In the Top Option bar, click *Connected*.
   b. Select the alias of the desired target device, then click *Disconnect*.

NOTE: For RASII target devices, the vKVM session interface and vMedia session interface are in the same page.

NOTE: After a DirectCommand connection, the target device may return unexpected results due to service processor instability. If this occurs, reset the service processor by connecting to the service processor console from the *Console - SP Console* menu and running the reset service processor command. The reset service processor command varies for each target device type; for example, for RSAII devices, the reset service processor command is **resetsp**. See *Device console and service processor console* on page 58 and *Profile Configuration* on page 131.

Direct access to service processor applications through Native IP (MergePoint 5224/5240 appliances only)

For target devices that do not support DirectCommand, administrators can enable Native IP on a MergePoint 5224/5240 appliances to allow access to native applications on the service processor. These applications are proprietary interfaces or command lines provided by the service processor vendor; examples include HP InSight, IBM Director and Dell Open Manage®. Enabling and configuring Native IP allows external user traffic to selectively pass through the MergePoint 5224/5240 appliance and directly connect to a service processor on the internal server network. Users can then bypass the MergePoint SP manager web interface and access the native interface on a service processor.

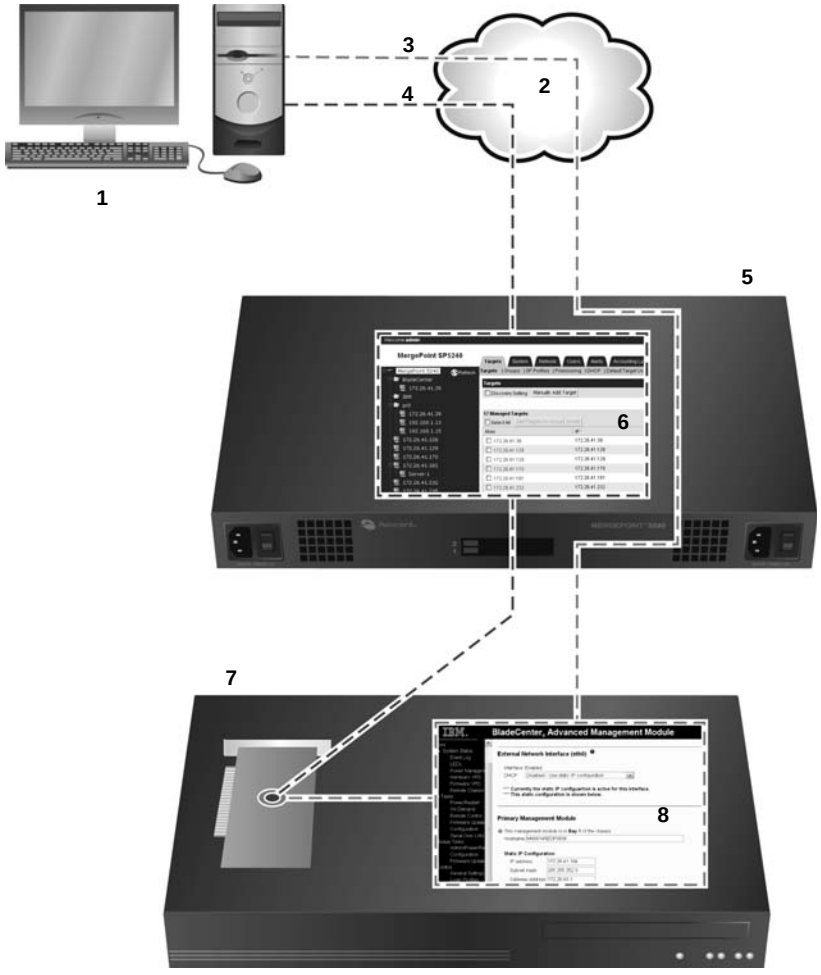


Figure 3.2: MergePoint 5224/5240 SP Manager Native IP Configuration

Table 3.2: Descriptions for MergePoint 5224/5240 SP Manager Native IP Configuration

Number	Description	Number	Description
1	Remote user	**5**	MergePoint 5224/5240 appliance
2	LAN	**6**	MergePoint SP manager web interface
3	Native IP connection to the service processor	**7**	Target device (service processor)
4	Connection to the MergePoint SP manager web interface	**8**	Native IP interface on the target device

To enable Native IP, you can enable selective mode or define Native IP trusts. The IP addresses in the trust are permitted to establish native IP connections.

To enable Native IP by enabling selective mode or creating Native IP trusts:

To enable selective mode, click *Network - Native IP Connects*. The Selective Mode status is displayed. Click *Start*.

-or-

To create a Native IP trust, click *Network - Native IP Trusts*.

a. Click *Add.*
b. In the IP field, enter a Native IP address range.
c. The Native IP trust address should be the address of the subnet itself, which means all of the host bits of the address are 0 (zero).
d. Enter a netmask and select an interface for the Native IP.
e. Click *Apply*.

To delete a Native IP trust:

1. Click *Network - Native IP Trusts*.
2. Select the Native IP you want to delete and click *Delete*.

To set up a Native IP connection:

1. Click *Network - Native IP Connects*.
2. Click *Add.*
3. In the Client IP field, type a host IP address.
4. In the Targets drop-down menu, select a service processor IP address.
5. Click *Apply.*

NOTE: The client IP address must be within a range of the Native IP trust. You must enable the Native IP connection in the service processor or create a permanent Native IP connection in the Native IP Connection tab.

To delete a permanent Native IP connection:

1. Click *Network - Native IP Connects*.
2. Select a Native IP connection.
3. Click *Delete*.

To enable or disable a service processor Native IP:

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, click *Native IP.* The Native IP window appears.

4. Click *Enable/Disable* to enable or disable Native IP.

NOTE: If the specified range of target device IP addresses is not included in a Native IP trust, the Native IP status is unavailable.

NOTE: A Native IP connection must be set up on a trusted network interface (specified when creating a Native IP trust).

To access the Native IP interface:

1. In the side navigation bar, click a target device name.
2. Click the *Configuration* tab.
3. In the top navigation bar, click *Native IP*, then click *Go to native IP interface*.

NOTE: Before access the Native IP interface, make sure you have already added a route or set the appliance as the default gateway for the host.

NOTE: The Go to native IP interface option is not visible if Native IP is not enabled.

For SSH commands that can be entered in the Native IP interface, see *SSH Commands for Native IP* on page 80.

Appliance Operations

MergePoint SP manager sessions

By selecting the *System - Sessions* option, the Admin user can view and manage MergePoint SP manager sessions and SSH/Telnet sessions.

Current MergePoint SP manager sessions are listed in the upper table of the session window.

To activate the session window and view a session:

Click *System - Session*. The current user session will be listed in green text.

To delete a session:

1. Click *System – Session.*
2. Select the session you wish to delete and click *Delete*.

Upgrade

Visit **www.avocent.com** to download and save the latest MergePoint SP manager upgrade firmware files onto your workstation.

To upgrade firmware on the MergePoint SP manager (Admin users only):

1. Click *System - Upgrade*.
2. In the Filename field, type the path to the firmware file or click *Browse* to locate the file.
3. Click *Upgrade*.

NOTE: If the upgrade fails, you may use the serial port to restore the MergePoint SP manager to the previous firmware version. For more information see *Enabling Web Interface Access* on page 12.

Boot configuration for MergePoint 5224/5240 appliance

By default, the MergePoint SP manager boots from an image file that resides on the Flash memory. The Boot from drop-down menu lists additional options for booting the MergePoint SP manager.

NOTE: Booting from the image file is strongly recommended. Network boots should be reserved only for troubleshooting or when you want to reinstall the firmware by first booting from a new image and then later writing it to the Flash memory.

Local boot options

To understand the local options on the Unit boot from menu, you need to understand how the MergePoint 5224/5240 appliance handles software upgrades:

- The MergePoint SP manager initially boots from a software image referred to as Image1.
- A new software version is downloaded and installed, the new image is stored as Image2 in the Flash memory and the configuration is changed so the MergePoint SP manager boots from Image2.
- Subsequent downloads are stored as Image1 and the configuration is changed so the MergePoint SP manager boots from Image1.

In the Unit boot from drop-down menu, the entry for the current boot image is selected by default.

After a software upgrade, the boot file location choices are:

- Network
- ImageN:image_filename

The word “image” is followed by the number, followed by a colon (:), followed by the name of the file, including the version number. The menu item has the following format:

imageN: uImage.<version>-<build date>

Network boot options

For a network boot, the following prerequisites must be met.

- A TFTP server must be available to the MergePoint SP manager.
- An upgraded boot image file must be available on the boot server.
- The MergePoint SP manager must have a fixed IP address.

Configuring boot characteristics

The boot configuration feature allows the Admin user to configure the MergePoint 5224/5240 appliance boot characteristics, including the location of the MergePoint SP manager boot file, the watchdog timer state, the console speed and the speed of the Ethernet interfaces.

To configure boot options (Admin users only):

1. Click *System - Boot configuration*.
2. In the Appliance IP Address field, type the IP address for the MergePoint SP manager.
3. In the Watchdog Timer drop-down menu, select Active or Inactive option as you desire.

NOTE: If the watchdog timer is active, the MergePoint SP manager reboots if the software crashes.

4. In the Unit boot from drop-down menu, select the desired boot method.
5. To configure the unit boot from network:
   a. Enter the filename of the network boot program in the Network boot filename field.
   b. Enter the IP address of the TFTP server in the Server's IP address field.
   c. Select your desired console speed from the Console speed drop-down menu.

NOTE: The Network boot file must be in the /tftpboot directory on the TFTP server.

6. Select the desired speed for the eth0 and eth1 interfaces from the menus provided.
7. Click *Apply.*

NOTE: The system reboots automatically after you change the Unit boot file and apply it.

Unbinding the MergePoint SP manager from the DSView 3 server

To unbind the MergePoint SP manager from the DSView 3 server:

1. Click *System - Advanced Setting*.
2. Click *Unbind from DSView 3 Server.*

CHAPTER 4

Configuring External Authentication Services

Configuring Authentication Services

By selecting the *Users – Authentication Services* menu option, the administrative user can configure authentication services. These authentication methods use both local authentication and authentication servers in the order shown: Local/AuthType, AuthType/Local and then AuthType Down/Local.

- The AuthType/Local and AuthType Down/Local authorization methods are referred to as authentication methods with local fallback options.
- Administrators can specify separate authentication types for the MergePoint appliance user accounts.
- Local authentication methods and the authentication methods that have local fallback options require user accounts configured on the MergePoint appliance.

If configuring any authentication method other than Local, the administrator user must make sure an authentication server is set up for that method as itemized in the following list.

- The appliance must have network access to an authentication server set up for every authentication method specified.
- Each authentication server must be configured and operational.
- The administrator configuring the appliance needs to work with the administrator of each authentication server to get user accounts set up and to obtain information needed for configuring access to the authentication server on the appliance.

The following table lists the supported authentication methods and their definitions.

Table 4.1: Supported Authentication Methods

Method	Definition
Local	Use local user/password for local authentication on the MergePoint appliance.
AuthType	Use user/password configured on the AuthType authentication server. No logins allowed if the AuthType server is down or the AuthType authentication fails.
AuthType Down/Local	Use local authentication if the AuthType server is down.

Table 4.1: Supported Authentication Methods (Continued)

Method	Definition
AuthType/Local	Use local authentication if the AuthType authentication fails.
Local/AuthType	Use the AuthType authentication if local authentication fails.

NOTE: The AuthType is Kerberos, LDAP, NIS, RADIUS, SMB, TACACS+ or DSView. For the DSView authentication method, the MergePoint appliance must be managed by the DSView 3 management software; otherwise, the DSView authentication will fail.

The default authentication service type is Kerberos. If any other authentication method is selected, additional fields appear on the screen for specifying the information for an authentication service of the selected method.

When the administrative user configures an authentication server on this page, the server is available to perform authentication checking for logins to the MergePoint SP manager, if the MergePoint SP manager is subsequently configured to use that authentication method. See *Configuring an authentication method for the MergePoint SP manager* on page 76 for how the MergePoint SP manager is assigned an authentication method.

Configuring a Kerberos authentication server

You need to configure a Kerberos authentication server when the MergePoint SP manager is configured to use the Kerberos authentication method or any of its variations (Kerberos, Local/Kerberos, Kerberos/Local or Kerberos Down/Local).

If the Kerberos authentication server (which is also referred to as a Key Distribution Center, or KDC) has previously been configured in either of the authentication configuration screens, the fields are filled in with the previously configured values.

NOTE: The Kerberos KDC rejects tickets when the timestamp on an authentication request from a host is not within the maximum clock skew time specified in the KDC's hdc.conf file. Therefore, it is essential for the time on the MergePoint SP manager to be synchronized with the time on the KDC.

To configure a Kerberos authentication server:

1. Make sure entries for the appliance and the Kerberos server exist in the MergePoint SP manager's /etc/hosts file.
   a. Select the *Network - Host Table* menu option. The Host Table form appears.
   b. Add an entry for appliance (if needed) and add an entry for the Kerberos server.
2. Make sure that time zone and time and date settings are synchronized between the MergePoint SP manager and on the Kerberos server.

NOTE: Kerberos authentication depends on time synchronization. Time and date synchronization is most easily achieved by setting both the MergePoint SP manager and the Kerberos server to use the same NTP server.

a. Follow the procedure to set the time zone, date and time.

b. Work with the authentication server's administrator to synchronize the time and date between the MergePoint SP manager and the server.

3. Click the *Users* tab.
4. In the top navigation bar, click *Authentication Services*. The Authentication Service Configuration window appears.
5. Select *Kerberos* from the Authentication Method drop-down menu. The Kerberos configuration fields display.
6. In the Kerberos Realm Domain Name field, type the domain name of the Kerberos.
7. In the Kerberos Server field, type the IP address of the Kerberos server.
8. Click *Apply*.

Configuring an LDAP authentication server

You need to configure a LDAP authentication server when the MergePoint SP manager is configured to use the LDAP authentication method or any of its variations (Local/LDAP, LDAP/Local or LDAP Down Local). See *Configuring group authorization for LDAP authentication* on page 87 for how to manually configure group authorizations with LDAP authentication.

To configure an LDAP authentication server:

1. Click the *Users* tab.
2. In the top navigation bar, click *Authentication Services*. The Authentication Service Configuration window appears.
3. Select *LDAP* from the Authentication Method drop-down menu. The LDAP form displays with LDAP Server and LDAP Base fields filled in from the current values in the /etc/ldap.conf file.
4. In the LDAP Server field, type the IP address of the LDAP server.
5. In the LDAP Base field, change the definition if the LDAP authentication server uses a different distinguished name for the search base than the one displayed.

NOTE: The default distinguished name is dc, as in dc=value,dc=value. For example, if the distinguished name on the LDAP server is o, then replace dc in the base field with o, as in o=value,o=value.

6. From the Secure LDAP drop-down menu, select either *Off*, *On* and *Start TLS*.
7. In the LDAP User Name field, type an optional username.
8. In the LDAP Password field, type an optional password.
9. In the LDAP Login Attribute field, type an optional login attribute.
10. Click *Apply*. The changes are stored in /etc/ldap.conf on the MergePoint SP manager.

Configuring an NIS authentication server

You need to configure an NIS authentication server when the MergePoint SP manager is configured to use the NIS authentication method or any of its variations (NIS/DownLocal, Local/NIS or NIS/Local).

To configure an NIS authentication server:

1. Click the *Users* tab.
2. In the top navigation bar, click *Authentication Services*. The Authentication Service Configuration window appears.
3. Select *NIS* from the Authentication Method drop-down menu. The NIS fields display.
4. In the NIS Domain Name field, type the NIS domain name.
5. In the NIS Server IP field, type the IP address of the NIS server.
6. Click *Apply.*

Configuring a RADIUS authentication server

You need to configure a RADIUS authentication server when the MergePoint SP manager is configured to use the RADIUS authentication method or any of its variations (Local/Radius, Radius/Local or Radius Down/Local). See *Configuring group authorization for RADIUS authentication* on page 90 for how to manually configure group authorizations with RADIUS authentication.

To configure a RADIUS authentication server:

1. Click the *Users* tab.
2. In the top navigation bar, click *Authentication Services*. The Authentication Service Configuration window appears.
3. Select *Radius* from the Authentication Method drop-down menu.
4. In the First Authentication Server field, type the IP address of the first or only authentication server.
5. In the Second Authentication Server field, type the IP address of a second authentication server (if available)
6. In the First Accounting Server field, type the IP address of the first or only accounting server.
7. In the Second Accounting Server field, type the IP address of a second accounting server (if available)
8. In the Secret field, type the secret.
9. In the Timeout field, type one or more time-out values.
10. In the Retries field, type a number of retries.
11. Click *Apply.*

Configuring an SMB authentication server

You need to configure an SMB authentication server when the MergePoint SP manager is to use the SMB authentication method or any of its variations (Local/SMB, SMB/Local or SMB Down/Local).

To configure an SMB authentication server:

1. Click the *Users* tab.
2. In the top navigation bar, click *Authentication Services*. The Authentication Service Configuration window appears.
3. Select *SMB* from the Authentication Method drop-down menu.
4. In the Domain field, type the SMB domain name.
5. In the Primary Domain Controller field, type the IP address of the primary domain controller.
6. In the Secondary Domain Controller field, type the IP address of the secondary domain controller.
7. Click *Apply*.

Configuring a TACACS+ authentication server

You need to configure a TACACS+ authentication server when the MergePoint SP manager is to use the TACACS+ authentication method or any of its variations (Local/TACACS+, TACACS+/Local or TACACS+ Down/Local). To configure a TACACS+ authentication server, you must prepare an account for admin or other admin user.

To configure a TACACS+ authentication server:

1. Click the *Users* tab.
2. In the top navigation bar, click *Authentication Services*. The Authentication Service Configuration window appears.
3. Select *TACACS+* from the Authentication Method drop-down menu.
4. In the First Authentication Server field, type the IP address of the first authentication server.
5. In the Second Authentication Server field, type the IP address of a second authentication server.
6. In the First Accounting Server field, type the IP address of the first accounting server.
7. In the Second Accounting Server field, type the IP address of the second accounting server.
8. In the Secret field, type the secret.
9. Check or leave unchecked the *Enable Raccess Authorization* checkbox.
10. In the Timeout field, type one or more time-out values.
11. In the Retries field, type a number of retries.
12. Click *Apply*.

Configuring an authentication method for the MergePoint SP manager

By selecting the Users-Authentication menu option, the administrative user can configure the authentication method that applies when anyone attempts to log into the MergePoint SP manager.

By default, Local authentication is in effect and no configuration is required.

The specified type of authentication server must be available and must be configured as described under *Configuring Groups for Use with Authentication Servers* on page 87.

To configure an authentication method for MergePoint SP manager logins:

1. Click the *Users* tab.
2. In the top navigation bar, click *Authentication*. The Authentication Configuration window appears.
3. Select the desired authentication method from the Authentication Method drop-down menu.
4. Click *Apply.*

CHAPTER 5

Administration Tasks Not Performed in the Web Interface

This section lists the configuration and maintenance tasks that are performed by an administrator (the root user, the admin user or a member of the admin group) either on the Linux command line, using the CLI utility or in the UBoot monitor mode.

Using MindTerm to Create an SSH Tunnel

This section describes how an admin user can create an SSH tunnel from a user workstation to a managed device using the MindTerm applet that activates when any user connects to the console using the web interface. A regular user cannot use this procedure; the Tunnels option is not available for them on the MindTerm menu.

NOTE: You must enable the SSH protocol before creating an SSH tunnel. See *Configuring the MergePoint SP Manager System* on page 34.

To use MindTerm to create an SSH tunnel:

1. Log into the web interface as an administrative user, and select *System – Setting*.
2. Select *Connect.* A window running a MindTerm applet appears, with an encrypted SSH connection between the user's computer and the console.
3. Log in and follow any prompts that may appear about saving the host key.
4. Press **Ctrl** and the right mouse button at the same time (**Ctrl**+[mouse right-click]) then drag the cursor to pull down and select the *Tunnels Basic* menu option.
5. The MindTerm Basic Tunnels Setup dialog box appears.
6. Enter a TCP port number to forward in the Local port field. You can select a random number over 1000.
7. Enter the device's port number to bring up the desired web application in the Remote port field.
8. Enter the IP address of the device in the Remote Host field.
9. Click *Add*. The tunnel is created and the dialog box appears similar to the following screen example.

Figure 5.1: MindTerm Basic Tunnels Setup Dialog Box

Using SSH with the MergePoint SP Manager

Both SSH v1 and SSH v2 services are supported on the MergePoint SP manager. The administrator may disable either version; if only one version of SSH is enabled, authorized users can use only a client running the same version.

If SSH is enabled, authorized users can use SSH in the following ways:

- Accessing the MergePoint SP manager console using an SSH client or SSH command, then connecting through the MergePoint SP manager to perform device management actions. See *User shell* on page 79 and *MgpShell* on page 80.
- Using the SSH command with special device management commands to perform device management actions without having to log into the MergePoint SP manager first. See *SSH Passthrough commands* on page 82.

To create an SSH connection:

1. Click *System - Setting*.
2. Click *Connect*. This connection uses the SSH protocol and opens in a separate window.

NOTE: See *Using MindTerm to Create an SSH Tunnel* on page 77 for more information.

The SSH command line format

The general format of the SSH command line is shown in the following example:

```
admin@MergePoint:~$ ssh -t
username:[devicename]@MergePoint_IP_or_DNS_name
```

In this example, the -t option is required to launch an interactive session. The username is the account name of the authorized user. The device name is the name/alias that was assigned to the device by the MergePoint SP manager administrator (used only when accessing a device).

To access the MergePoint SP manager console, omit the device name:

```
admin@MergePoint:~$ ssh -t admin:@MergePoint_IP_or_DNS_name
```

The MergePoint_IP_or_DNS_name is the IP address of the MergePoint SP manager or its DNS name. The command is one of the MergePoint SP manager specific device management commands described in the SSH Passthrough table.

User shell

After logging in the MergePoint SP manager console via SSH command or SSH applications (such as Putty or Telnet) non-admin users see a menu like the one shown in the following example.

```
Access Devices

Change Password

Logout
```

Admin users can get to the same menu either by entering the **rmenush** command on the SSH command line or by entering **/usr/bin/rmenush** on the command line after login. You can move from one item to another on the menu and submenus by using the keyboard arrow keys. A line (-) appears next to the selected item.

When Access Devices is selected, a menu appears with a list of devices that the user is authorized to access. After a device is selected, pressing the **Enter** or **Return** key brings up the list of actions the user is authorized to perform on the device.

Not all listed actions are supported for all service processors. The following example shows the service processor action menu for an HP iLO/iLO2 service processor.

```
HP iLO/iLO2

Access the service processor's console

Access the device's console via SoL

Manage power

Reset SP

Manage the event log

View sensor output

Start Telnet session

Start SSH session

Enable native IP

Disable native IP
```

```
Exit
Back
```

NOTE: If you select *Start Telnet session* or *Start SSH session,* you are prompted for the corresponding port, and then required to enter the username and password.

NOTE: The Enable native IP and Disable native IP commands are only supported on the MergePoint 5224/5240 appliance.

MgpShell

After logging in MergePoint SP manager console via SSH command or SSH applications as an admin user, typing **mgpshell** and pressing the **Enter** or **Return** key brings up a list of devices you are authorized to access, as shown in the following example.

```
Select a device
IBM Blade Center
HP Blade System
HP iLO/iLO2
Exit
```

After a device is selected, a submenu lists the device management actions available to the user. See *User shell* on page 79 for details.

SSH Commands for Native IP

Admin users can create Native IP trusts and open Native IP connections with SSH commands. Admin users can specify what IP addresses from which interfaces are trusted to bring up direct connection to service processors.

To login to the MergePoint appliance console as admin user:

You may log in to the MergePoint appliance with any of the SSH clients, such as PuTTY tool, SecureCRT tool or OpenSSH client. The following command examples use the OpenSSH client under a Linux terminal.

Run the command by entering the following: `admin@MergePoint:~$ **ssh -t username@MergePoint_IP_or_DNS_name**`

For example:

`admin@MergePoint:~$ **ssh -t admin@172.26.25.173**`

To enable selective mode:

Run the command by entering the following: `admin@MergePoint:~$ **nativeipctl truston 0.0.0.0/0.0.0.0**`

To add a Native IP trust:

Run the command by entering the following: `admin@MergePoint:~$` **`nativeipctl truston <native_IP_Trust>/<netmask> dev <interface>`**

For example, to allow direct connection from 172.X.X.X network segment to service processors:

`admin@MergePoint:~$` **`nativeipctl truston 172.0.0.0/255.0.0.0 dev eth0`**

For example, to allow direct connection from host 192.168.0.1 to service processors:

`admin@MergePoint:~$` **`nativeipctl truston 192.168.0.1/255.255.255.255 dev eth0`**

NOTE: The parameter dev defines the interface that all the connections should go through. If the interface is eth0, then only the connections through eth0 are allowed to be set up.

To list all the available trusts by command:

Run the command by entering the following: `admin@MergePoint:~$` **`nativeipctl list trusts`**

To enable Native IP connection (Temporarily):

Run the command by entering the following: `admin@MergePoint:~$` **`nativeipctl on client <host ip address> <device IP address>`**

For example, to enable temporarily direct access from 172.26.27.15 to 172.26.25.160:

`admin@MergePoint:~$` **`nativeipctl on client 172.26.27.15 172.26.25.160`**

To disable Native IP connection (Temporarily):

Run the command by entering the following: `admin@MergePoint:~$` **`nativeipctl off type t client <host ip address> <device IP address>`**

To enable Native IP connection (Permanently):

Run the command by entering the following: `admin@MergePoint:~$` **`nativeipctl on type p client <host ip address> <device IP address>`**

For example, to enable permanently direct access from 12.23.56.78 to 172.26.25.157:

Run the command by entering the following: `admin@MergePoint:~$` **`nativeipctl on type p client 12.34.56.78 172.26.25.157`**

To disable Native IP connection (Permanently):

Run the command by entering the following: `admin@MergePoint:~$` **`nativeipctl off type p client <host ip address> <device IP address>`**

To list all the available Native IP connections:

Run the command by entering the following: `admin@MergePoint:~$` **`nativeipctl list connections`**

SSH Passthrough

SSH Passthrough allows you to perform management operations on target devices without having to log into the MergePoint SP manager first. You may establish an SSH connection to a target device by specifying the appropriate name in the SSH command. When opening an SSH passthrough connection to a supported device, you may include an service processor command at the end of the SSH command. If the service processor command is not present at the end of the SSH command, the MergePoint SP manager will provide the user with a menu of service processor commands to choose from.

SSH Passthrough commands

There are two types of SSH commands: commands without an service processor command and commands with an service processor command.

To access a target device through SSH Passthrough:

Run the command by entering the following: **`ssh –t userA:serverB@applianceC`**.

NOTE: In this example, a user (userA) is trying to access a target device (serverB) that is connected to a MergePoint SP manager (applianceC).

This command allows the user to get access to serverB's service processor. A menu appears after successfully logging in. The user can manage serverB by choosing a menu item.

To access a target device through SSH Passthrough with service processor command:

Run the command by entering the following: **`ssh –t userA:serverB@applianceC [command]`**.

NOTE: In this example, a user (userA) is trying to access the service processor feature [command] on a target device (serverB) that is connected to a MergePoint SP manager (applianceC).

The first part of the command will establish an SSH session to the MergePoint SP manager. The command is passed through to the service processor connected to the MergePoint SP manager. The MergePoint SP manager will validate and execute the command.

For example, a command to open an SSH session to the MergePoint SP manager and execute power on command may look like this:

```
ssh –t jsmith:MGP@172.30.19.122 poweron
```

Table 5.1: Supported Service Processor Commands

Command Name	Description
clearsel	Clears the target device SEL.

Table 5.1: Supported Service Processor Commands (Continued)

Command Name	Description
devconsole	Opens SoL for the target device.
nativeipoff	Rrevokes direct access to the service processor. **NOTE:** This command is only supported on the MergePoint 5224/5240 appliance.
nativeipon	Configures the appliance to allow direct access to the service processor. **NOTE:** This command is only supported on the MergePoint 5224/5240 appliance.
powercycle	Turns off a target device that is turned on, then after 10 seconds turns it on again.
poweroff	Turns the target device off.
poweron	Turns the target device on.
powerstatus	Shows the power status of the target device.
reset	Restarts a target device that is turned on.
sel	Views the target device SEL.
sensors	Views the sensor status of a target device.
solhistory	Displays the history of the console on the managed server.
solreplay	Replays the history of the console on the managed server.
spconsole	Accesses the command line on the service processor.
spconsole <action>	Executes the specified action on the service processor, then exits.
ssh	Starts an SSH session on the server.
telnet	Starts a Telnet session on the server.

Telnet

You can start or stop the Telnet service at any time.

To start or stop Telnet service:

1. Log into the MergePoint SP manager console as **root**.
2. Edit the Telnet file using the following command:

   ```
   root@Mergepoint:~# vi /etc/xinetd.d/telnet
   ```

3. Set the value of "disable" to "yes" or “no” to disable or enable the Telnet service.
4. Quit vi and run the following command to apply the setting and restart the Telnet service.

   ```
   root@Mergepoint:~# /etc/init.d/xinetd restart
   ```

NOTE: You can also enable or disable Telnet in the System - Settings window in the web interface. See *Configuring the MergePoint SP Manager System* on page 34.

Configuring the Users' Console Login Menu

Regular users are configured with /usr/bin/rmenush as their default login shell. All users with rmenush as their login shell see the same menu whenever they log into the console.

The MergePoint SP manager administrator can configure the rmenush menu to display other options including links to additional submenus or commands by modifying the /etc/menu.ini file.

NOTE: If changing the default menu, the administrator must ensure that any added programs do not introduce security vulnerabilities.

The administrator must know the following about the behavior of rmenush before configuring any changes to the menu:

- If the called program exits with a return code indicating an error, rmenush prompts the user to press any key to continue.
- Any error messages generated by the called program are left on the screen for the user to read. Examples showing how the administrator can force this behavior on for successful programs and off for unsuccessful ones are provided in the configuration file.
- The MergePoint SP manager administrator assigns the /usr/bin/rmenush shell to users as appropriate, by editing the /etc/passwd file entries for the users.

When editing the menu.ini file, the administrator must know the following:

- Spaces are shown in menu items by the use of an underscore between words.
- An underscore cannot be displayed in the menu text.
- The righthand value of each name/command pair is assumed to be either a menu defined in the menu.ini file or a command.
- A maximum of 16 menu items can display on the screen at a time. Any extra menu items can be reached by using the arrow keys to scroll down.

To modify the user shell menu:

See *root@Mergepoint:~# /etc/init.d/xinetd restart* on page 83 for background information and examples.

NOTE: When adding programs to the menu, make sure the commands do not allow the user to break out of the programs they call.

1. Log into the MergePoint SP manager console as **root**.
2. Open the /etc/menu.ini file for editing.

3. Add new menus and menu items as desired, using underscores (_) to indicate spaces between words. In the [main] menu definition, insert a definition for an action or an option for a submenu, as desired. The following example shows a new menu option with a command defined along with a link to a new subnet identified with the new submenu keyword.

```
[main]
Access_Servers = /bin/spshell
Change_Password = /usr/bin/passwd
New_Menu_Option = command_pathname_and_options
New_Submenu = newsubmenu
```

4. Add a definition for a submenu using the defined keyword by entering the following:

```
[newsubmenu]
Submenu_Option1 = command_pathname_and_options
Submenu_Option2 = command_pathname_and_options
```

5. Save and quit the file.

Configuring Routes With CLI

The following procedures give examples for using the CLI utility for configuring default, host and network routes and assigning them to interfaces or to gateways.

NOTE: Setting a gateway IP address automatically creates a default route to the gateway's IP address.

To configure routes with CLI:

1. Log into the console as **root**.
2. Enter the **cli** command.
3. Set network interface by entering the following:

```
cli> set network interface <interface_name> address <IP_address>
OK
```

4. Set a default route by setting a gateway IP address by entering the following:

```
cli> set network interface <interface_name> gateway <gatewayIP>
OK
```

5. Add a host in the host table by entering the host's IP address after the **add network hosts** command.

```
cli> add network hosts <hostIP> name <hostname> alias <alias>
```

6. Add a network route by entering the network address after the **add network st_routes** command in the form 1.2.3.0/24.

```
cli> add network st_routes <networkIP/NN>

OK
```

7. For both host and network routes, use the **set network st_routes** command to assign the route to an interface or to a gateway and optionally assign it a metric, by performing the following steps.

   To assign the route to an interface, enter **set network st_routes <IPaddress | networkIPaddress/NN> device <ethN>**. The following screen example shows assigning the host route created in step 5 to the device eth0 and assigning an optional metric.

   ```
   cli> set network st_routes <IPaddress|networkIPaddress/NN> device eth0
   metric <N>

   OK
   ```

   -or-

   To assign the route to a gateway, enter **set network st_routes <IPaddress | networkIPaddress/NN> gateway <gatewayIP>**. The following screen example shows assigning the network route created in step 6 to the gateway 192.168.2.0.

   ```
   cli> set network st_routes <IPaddress|networkIPaddress/NN> gateway
   192.168.2.0

   OK
   ```

Backing Up Configuration Files

MergePoint SP manager administrators can create a compressed backup of all configuration files and store the backup in a specific file. Any compressed configuration file that already resides in the directory is overwritten. The following procedure shows how administrators can back up configuration files in different environments on the MergePoint SP manager.

To back up configuration files:

1. If you are logged into the web interface as an administrative user, select *System -Import/Export* and click *Export*.
2. If you are logged into the console as the root user, enter the following **saveconf** command:

   ```
   root@MergePoint:~# saveconf <filename>
   ```

Restoring backed up configuration files

To perform this procedure, a previous administrator must have previously either run the saveconf command or selected *System - Import/Export* and clicked *Export*, saving changes to the configuration. This procedure restores the configuration files to the state they were in when they were last backed up.

To restore the configuration files to the last saved version:

1. If you are logged into the web interface as an administrative user, select *System -Import/Export* and click *Import*.
2. If you are logged into the console as the root user, enter the **restoreconf** command:

```
root@MergePoint:~# restoreconf <filename>
```

Restoring factory default configuration files

A root user can restore the factory default configuration files from a specific file by performing the following procedure while logged in through the console, Telnet or SSH to restore the configuration files to the state they were in when the MergePoint SP manager shipped. For how to restore factory defaults while you are saving a boot image from RAM memory onto the resident Flash memory, see *To upgrade to a boot image from a network boot:* on page 144.

To restore the factory default configuration files from the command line:

Log into the console as the root user and enter the **restorefactory** command:

```
root@MergePoint:~# restorefactory
```

Configuring Groups for Use with Authentication Servers

This section applies when an authentication method that relies on an authentication server is configured for the MergePoint SP manager. If the administrator of an authentication server configures users as members of groups as described in this section, the users do not need to have accounts configured on the MergePoint SP manager.

For example, user johnb is defined as a member of the admin group on a TACACS+ server, but does not have a user account on the MergePoint SP manager. If the MergePoint SP manager is configured for TACACS+ authentication, johnb can log into the MergePoint SP manager as an adminstrator.

To support the use of groups with the authentication methods that support groups, the administrator must configure local groups on the MergePoint SP manager using the same group names used on the authentication servers, using the web interface or the CLI utility.

The admin group exists by default. User accounts do not need to be configured on the MergePoint SP manager for the users in the authentication server defined groups.

Configuring group authorization for LDAP authentication

Group authorizations can be provided by either a Windows Active Directory (AD) server or a server running OpenLDAP:

- On an AD server, the info attribute can be used to define groups, but the memberOf attribute is already used in the AD schema to denote domain membership and so it cannot be used to defining groups.

- On an OpenLDAP server, either the info attribute or memberof attribute can be used.

Configuring group authorizations on an AD server

Perform the following procedures for configuring support for group authorizations when a Windows Active Directory server is used for LDAP authentication.

To install Windows Administration Pack tools and configure the snapin:

1. On the server, install the tools from the Windows Administration Pack. The tools are found on the Windows server installation CD.
2. Go to the start menu and click *Run*.
3. In the Open field, type **mmc /a** and click *OK*. A console window appears.
4. Click *Console* in the console window menu bar and select *Add/Remove Snapin.* The Add/Remove Snapin window appears.
5. Click *Add*. The Add Standalone Snapins window appears.
6. Select *Active Directory Schema* from the list of snapins and click *Add*.
7. Select *ADSI Edit* from the list of snapins and click *Add*.
8. Click *Close*, then click *OK* in the Add/Remove Snapin window.

To configure Active Directory schema:

1. In the server's console window, double-click *Active Directory Schema*. The paths Classes and Attributes appear.
2. Double-click *Attributes* and confirm that the info attribute is present.
3. Double-click *Classes*, locate the class Users and right-click to select *Properties*.
4. Select the *Attributes* tab and click *Add*.
5. Locate info in the attributes list. Click *Apply*, then click *OK*

To configure a group in ADSI Edit:

1. In the server's console window, double-click *ADSI Edit*.
2. From the menu, select *Action Connect to.* The Connection window appears.
3. Accept the defaults and select *OK*.
4. The path Domain NC<domain>.com appears.
5. Double-click *Domain NC<domain>.com.* The expanded path DC=*xxx*,DC=*xxx*,DC=com appears.
6. Double-click *DC=xxx,DC=xxx,DC=com*.
7. The expanded class CN=Builtin appears.
8. Double-click *CN=Users*. The expanded users list appears.
9. Right-click on the name of a user and select *Properties*. The CN=<username> Properties window appears.

10. In the Optional area, select which property to view: *locate* or *select [info]*.
11. In the Edit Attribute field, enter the group name in the format group_name=<Group1>. If the username selected is an administrative user, enter admin as the group_name.
12. Click *OK* and close or save the windows.

Defining groups on an LDAP server running OpenLDAP

Perform the following procedures for configuring support for group authorizations when a server running OpenLDAP is used for LDAP authentication.

Any groups configured in the memberof attribute are used; if no groups are defined in the member of attribute, then any groups configured in the info attribute are used. The groups defined on the LDAP server must be configured on the MergePoint SP manager with the desired device access authorizations.

To configure groups using the info attribute on an LDAP authentication server:

1. On the server, add the info attribute into the objectclass posixAccount in the /etc/ldap/schema/nis.schema file:

   ```
   objectclass (1.3.6.1.1.2.0 NAME 'posixAccount' SUP top AUXILIARY DESC
   'Abstraction of an account with POSIX attributes' MUST ( cn $ uid $
   uidNumber $ gidNumber $ homeDirectory ) MAY ( userPassword $ loginShell
   $ gecos $ description $ info) )
   ```

2. Make sure the info attribute exists in the /etc/ldap/schema/cosine.schema file.

   ```
   attributetype (0.9.2342.19200300.100.1.4 NAME 'info'
   DESC 'RFC1274: general information'
   EQUALITY caseIgnoreMatch
   SUBSTR caseIgnoreSubstringsMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{2048} )
   ```

   Make sure both schema files are listed in slapd.conf:

NOTE: The slapd.conf file is normally located in: [Redhat] /etc/openldap or [bsd] /usr/local/etc/openldap.

   ```
   include /etc/openldap/schema/nis.schema
   include /etc/openldap/schema/cosine.schema
   ```

3. Restart the LDAP service to activate changes.
4. Use the ldapadd(1) command to add new users or the ldapmodify(1)command to assign a user to one or more groups in one of the two following ways:
   a. Enter the user information including the group name or names on the command line, using the ldapadd command to add new users or the ldapmodify command to modify existing users.

b. Put all user information, including the group definition in a text file and use the text file with the f option on the command line to configure groups for users. Use the following syntax for configuring a group using the info attribute:

```
info: group_name=<Group1>[,<Group2>,...,<GroupN>];
```

NOTE: To give a user administrative access to the MergePoint SP manager, add the admin group name to the group_name definition.

To configure groups using the memberof attribute on an LDAP authentication server:

1. On the server, add the memberof attribute to the /etc/openldap/schema/core.schema file:

```
attributetype (1.2.840.113556.1.2.102 NAME 'memberof'
DESC 'Group membership'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12)
# Standard object classes from RFC2256
# RFC 2377
objectclass ( 1.3.6.1.1.3.1 NAME 'uidObject'
        DESC 'RFC2377: uid object'
        SUP top AUXILIARY MUST ( uid $ memberof) )
```

2. On the server, configure the group(s) assigned to each user with one entry for each group, either in a user definition file in the /etc/openldap directory, as shown in the following example, or on the command line.

```
dn: cn=<username>,dc=qa,dc=<domain>,dc=com
uid: <username>
cn: <username>
...
memberof: cn=<Group1>,dc=<domain>,dc=<domain>,dc=com
memberof: cn=d<Group2>,dc=<domain>,dc=<domain>,dc=com
memberof: cn=<Group3>,dc=<domain>,dc=<domain>,dc=com
...
homeDirectory: /home/<username>
```

NOTE: To give a user administrative access to the MergePoint SP manager, assign the admin group name in a memberof definition.

Configuring group authorization for RADIUS authentication

The two tasks listed below must be done to configure groups for RADIUS authentication.

- The RADIUS server's administrator must define the desired groups and assign users to the groups. See *To configure groups on a RADIUS authentication server:* on page 91.
- The MergePoint SP manager's administrator must configure the RADIUS server on the MergePoint SP manager. The following list defines the values to define when configuring a RADIUS authentication server on the MergePoint SP manager as shown below.

  `auth1 server[:port] secret [timeout] [retries]`

  `acct1 server[:port] secret [timeout] [retries]`

  The following list defines each of the values:

  - auth1: the first RADIUS authentication server
  - acct1: the first RADIUS accounting server
  - server: the RADIUS server address
  - port: (optional) the default port name is radius and is looked up through /etc/services.
  - secret: the shared password required for communication between the MergePoint SP manager and the RADIUS server
  - retries: the number of times each RADIUS server is tried before another is contacted
  - timeout: the default is 3 seconds. How long the MergePoint SP manager should wait for the RADIUS server's response.

To configure groups on a RADIUS authentication server:

1. On the server, open the /etc/raddb/users file for editing.
2. Assign groups to a user in the FramedFilterId attribute.
3. Use the format FramedFilterId=:group_name=<Group1>[,<Group2>,..., <GroupN>];, as shown in the following example:

```
groupuser1
AuthType= Local, Password =”xxxx”
ServiceType=CallbackFramedUser,
CallbackNumber=”305”,
FramedProtocol=PPP,
FramedFilterId=”:group_name=<Group1>[,<Group2>,..., <GroupN>];”,
FallThrough=No
```

NOTE: If the FrameFilterId already exists, append the group_name declaration to the string starting with a colon (:). Make sure a final semicolon (;) is at the end of the declaration, as shown in the example.

4. Save and quit the file.

To configure a RADIUS authentication server on the MergePoint SP manager:

1. Log into the console as the root user.

2. Open the /etc/raddb/server file for editing or create the file.
3. Make an entry for the RADIUS server (auth1), an accounting server (acct1) and make an entry for a second RADIUS authentication server (auth2) and for a second accounting server (acct2), by performing the following steps for each server.
4. Follow the file configuration directions shown in the following example.

```
# For proper security, this file SHOULD have permissions 0600,
# that is readable by root, and NO ONE else. If anyone other than
# root can read this file, then they can spoof responses from the
server!
# #
There are 3 fields per line in this file. There may be multiple
# lines. Blank lines or lines beginning with '#' are treated as
# comments, and are ignored. The fields are:
#
# server[:port] secret [timeout]
#
# the port name or number is optional. The default port name is
# "radius", and is looked up from /etc/services The timeout field is
# optional. The default timeout is 3 seconds.
#
# If multiple RADIUS server lines exist, they are tried in order. The
# first server to return success or failure causes the module to return
# success or failure. Only if a server fails to response is it skipped,
# and the next server in turn is used.
#
# The timeout field controls how many seconds the module waits before
# deciding that the server has failed to respond.
#
# server[:port] shared_secret timeout (s)
# 127.0.0.1 secret 1
# otherserver othersecret 3
OUR.RADIUS.SERVER.IP:1645 OurSecret 1 3
```

5. Enter the IP address for the server.
6. (Optional) Define an alternate port.

7. Enter the secret (shared password).
8. (Optional) Enter a value to redefine the timeout.
9. (Optional) Enter a value to redefine the number of retries. The following screen example shows entries that define the RADIUS authentication server and the accounting server to be the same server with the same IP address, sets the secret to avocent, the timeout to 5 seconds and the number of retries to 5.

```
auth1 172.20.0.2 avocent 5 5
acct1 172.20.0.2 avocent 5 5
```

NOTE: Always configure both parameters auth1 and acct1.

10. Save and quit the file.

NOTE: Multiple RADIUS servers can be configured in this file. The servers are tried in the order in which they appear. If a server fails to respond, the next configured server is tried.

Configuring group authorization for TACACS+ authentication

The two tasks listed below must be done to configure groups for TACACS+ authentication.

- The TACACS+ server's administrator must define the desired groups and assign users to the groups.
- The MergePoint SP manager administrator must configure the TACACS+ server on the MergePoint SP manager and set up the TACACS+ server for raw access. For more information see *Configuring a TACACS+ authentication server on the MergePoint SP manager* on page 94.

The following CLI utility command line can also be used to configure a server for raw access:

```
cli> set auth tacplus service raccess
```

To assign a group to a user on the TACACS+ server:

1. Add a definition for the group to the authentication authorization accounting (AAA) database on the TACACS+ server.

NOTE: These additions can be made through a GUI. The example shows the configuration if a GUI is not available.

```
############################################################
#  Group Definitions
############################################################
group = group_name {
...
}
```

2. To the definition for each user, add the raccess service in the form service = raccess and assign the desired group to the user in the form member = group_name.

NOTE: Each user may belong to only one group. To give a user administrative access to the MergePoint SP manager, assign the admin group.

```
############################################################
#  User Definitions
############################################################
user = username {
           service = raccess
               member = group_name
}
```

Configuring a TACACS+ authentication server on the MergePoint SP manager

The following list defines the values that must be defined in the MergePoint SP manager's /etc/tacplus.conf file.

- authhost1: IP address of the TACACS+ authentication server. A second TACACS+ authentication server can be configured with the parameter authhost2.
- accthost1: IP address of a TACACS+ accounting server, which can be used to track how long users are connected after being authorized by the authentication server. Its use is optional. If this parameter is not defined, accounting is not be performed. If the same server is used for authentication and accounting, both parameters must be defined with the same address. A second TACACS+ accounting server can be configured with the parameter accthost2.
- secret: The shared secret (password) necessary for communication between the MergePoint SP manager and the TACACS+ servers.
- encrypt: The default is 1, enable encryption. A value of 0 means disable encryption.
- service: The service to be enabled, in this case: raccess.
- protocol: The default is lcp (line control protocol). Specify another parameter if required.
- timeout: The timeout (in seconds) for a TACACS+ authentication query to be answered.
- retries: Defines the number of times a TACACS+ server is tried before another is contacted. The first server authhost1 is tried for the specified number of times, before the second authhost2, if configured, is contacted and tried for the specified number of times. If the second server fails to respond or if no second server is configured, TACACS+ authentication fails.

To configure a TACACS+ authentication server on the MergePoint SP manager:

1. Log into the console as **root**.
2. Open the /etc/tacplus.conf file for editing.

3. Change the values described under Configuring a TACACS+ authentication server on the MergePoint SP manager.

NOTE: To configure group access on the TACACS+ authentication server, the service must be defined as raccess.

4. Save and quit the file.

Switching the Port Speed in the MergePoint 5224/5240 Appliance

You may set a switch port speed individually, or retrieve the current port speed from the MergePoint 5224/5240 appliance.

To set the switch port speed:

1. Log into the MergePoint SP manager console as **root**.
2. Set the port speed using the following command:

```
Sysctl marvell.xxx=value
(Value = auto / 10f / 10h / 100f / 100h / 10F / 10H / 100F / 100H)
```

NOTE: The definitions for the values are:
- auto: Auto mode. The system selects an appropriate speed for the switch port.
- 10f / 10h / 100f / 100h: Mandatory mode. The system cannot change the value. This setting may cause operations to fail if the value is not appropriate for the switch port.
- 10F / 10H / 100F / 100H: Negotiable mode. System may use this value, or set another value if this value is not appropriate for the switch port.

To get the individual port speed:

1. Log into the MergePoint SP manager console as **root**.
2. Retrieve the current speech of the switch port using the following command:

```
sysctl –n marvell.xxx
```

NOTE: The xxx value is the switch port number. The output is the current speed of the switch port. The current speed may differ from the speed you set if you chose auto mode or negotiable mode for the speed value.

CHAPTER 6

Using the CLI Utility

CLI Utility Overview

An administrator can configure the MergePoint SP manager using the CLI utility. While in the CLI utility, an administrator can escape to the shell and when finished can return to the CLI utility.

Administrators often prefer using the CLI utility over the web interface because they can run frequently performed CLI configuration commands from shell scripts or from text files that can be executed in batch mode. For example, on a MergePoint SP manager with 40 private Ethernet ports, configuring all the service processors one by one could be tedious and prone to error, so scripting the configuration of multiple service processors at one time is a good use of the CLI utility.

The CLI utility provides a set of commands (described under see *CLI Commands* on page 102) that act on parameters nested in a format called the CLI parameter tree. Some parameters require arguments when the parameters are entered with some commands.

NOTE: This section describes the CLI commands and how to navigate the CLI parameter tree, but it does not describe all the parameters and values.

NOTE: In the examples in this section, the failover parameter in the /network/interface/mode directory is only for the MergePoint 5224/5240 appliance.

Execution Modes

The CLI utility has three modes: a command line mode, interactive mode and batch mode.

Command line mode

Command line mode refers to when the CLI utility is invoked on the Linux command line with options, commands, parameters and values.

The CLI utility performs the specified commands, displays any values requested by a command (such as the **get** command) and returns the shell prompt. To commit the changes made in command line mode, make sure to use the **-C** option as part of the command line. See *CLI Options* on page 98.

When invoked without commands, CLI enters interactive mode; see *Interactive mode* on page 98. When the CLI utility is invoked with the **-f <file>** option or is invoked from a script, the commands are executed in batch mode from the specified file or script. See *CLI Options* on page 98.

Interactive mode

Interactive mode is entered by invoking CLI on the command line. The cli> prompt appears, and the administrator performs configuration by entering commands followed by parameters followed by parameter arguments at the cli> prompt. The CLI utility waits for new commands until the user enters the **quit** or **exit** command.

Batch mode

Batch mode refers to invoking CLI commands from a file as follows:

CLI commands can be saved in a plain text file and executed in batch mode by invoking the CLI utility with the **-f <file>** option.

- CLI commands can be used in any kind of shell script:
  - **#!/usr/bin/cli** can be invoked at the top of a shell script if the script contains only CLI commands.
  - Any type of shell can be used to run CLI commands along with other commands.

CLI Options

Administrators can invoke the CLI command with a number of different options shown in the following table.

Table 6.1: CLI Utility Options

Option	Description
-1	Single command only (no effect in interactive mode).
-C	Commits changes automatically when quitting.
-f <file>	Reads commands from *<file>*. Used for running commands in batch mode. **NOTE:** You may use "**-**" for stdin, such as **cli -f -**.
-c <file>	Used for running *cli.conf* from *<file>* when *cli.conf* is not under the default path: **/etc/cacpd**.
-p <file>	Used for running *param.conf* from *<file>* when *param.conf* is not under the default path: **/etc/cacpd**.
-m <file>	Used for running *modules.conf* from *<file>* when *modules.conf* is not under the default path: **/etc/cacpd**.

Table 6.1: CLI Utility Options (Continued)

Option	Description
-h	Help. Shows a brief summary of command line options.
-q	Quiet mode; don't show the startup greeting.
-V	Show CLI version.

CLI Parameters and Arguments

The CLI configuration options are organized in a hierarchy called a parameter tree. You can use the **get**, **show** and **list** commands to show parameters. You can also use the **get** command to show the values of individual parameters at the end of a branch.

Each branch in the parameter tree in the MergePoint SP manager CLI is made up of one or more parameters, one nested below the other. For example, the toplevel network parameter may be followed by the secondlevel interface parameter, which then may be followed by the thirdlevel *mode* parameter. In this branch, the only commands supported would be **get** and **set**. All of the parameters in a branch are entered together on a single CLI command line. For example, to get the value, then set the mode for failover, you would enter the following command:

```
cli> get network interface mode
normal
cli>
```

To set failover, you would enter the following command in interactive mode:

```
cli> set network interface mode failover
OK
cli>
```

You can use autocompletion with the set command to find out the accepted values:

```
cli> set network interface mode <Tab><Tab>
Set interface mode: normal, interface or bridge.
```

To add a user called mozart, you would enter the following:

```
cli> add spmanager user mozart
OK
```

Entering a command in interactive mode

Based on the branch mentioned at the beginning of this section, you could enter the **set** command with the following parameters in interactive mode to turn on Ethernet failover.

```
admin@MergePoint:~$ cli
```

```
cli> set network interface mode failover
ok
cli>
```

Entering a command in command code

Based on the branch mentioned at the beginning of this section, you could enter the **set** command to turn on Ethernet failover with the parameters shown in the following screen example in command mode. When the command completes, the shell prompt returns. On the command line, you could enter all the parameters together with the value on the same command line.

```
admin@MergePoint:~$ cli -C1 set network interface mode failover
ok
admin@MergePoint:~$
```

Entering a command in batch mode

Based on the example in this section, you could use batch mode to turn on Ethernet failover as shown in the following examples.

Example CLI shell script

Start the script by entering **#!/usr/bin/cli** with the *-Cf* options:

```
#!/usr/bin/cli -Cf
set network interface mode failover
```

You could then make the script executable and execute it on the command line, as shown in the following example.

```
root@MergePoint:~$ chmod 777 scriptname1
root@MergePoint:~$ ./scriptname1
```

Example bash shell script

If you want to run a CLI command from the same script that is running other Linux commands, you could put the command in another type of shell script. The bash shell is shown in the following example:

```
#!/bin/bash
...
/usr/bin/cli -C set network interface mode failover
...
```

If you want to run multiple CLI commands from a script that is also running other Linux commands, you could add the multiple CLI commands as shown in the following example:

```
#!/bin/bash
```

```
...
/usr/bin/cli <<EOF
set network interface mode failover
set network hostname frutabaga
commit
EOF
```

You could then make the script executable and execute it on the command line, as shown in the following example:

```
root@MergePoint:~$ chmod 777 scriptname2
root@MergePoint:~$ ./scriptname2
```

Example plain text file

You can put one or more commands in a plain text file without invoking any shell as shown in the following example.

```
set network interface mode failover
```

Then you can invoke the CLI command with the **-f <file>** option to execute the command(s) from the file, as shown in the following example.

```
root@MergePoint:~$ cli -f filename
```

Autocompletion

Autocompletion can be used to find out what commands and parameters are available. Pressing the **Tab** key twice displays all the commands at the top level, as shown in the following screen example.

```
cli> <Tab><Tab>
add    commit   exit  list   rename    set   show
cd     delete   get   quit   revert    shell version
```

Typing any of the commands such as **add** or **set** then pressing **Tab** twice displays all the top level parameters, as shown in the following screen example.

```
cli> set<Tab><Tab>

adsap2        cards         network       snmpd         syslog
auth          dhcpd         ntp           spmanager     timezone
bootconf      iptables      pxe           sshd          tcpdump
```

Pressing **Tab** once after partially typing a parameter name automatically completes the parameter name, unless there is more than one parameter name beginning with the typed characters. If more than one parameter name begins with the typed characters, then **Tab Tab** displays them all.

NOTE: The **bootconf** and **cards** commands are only for MergePoint 5224/5240 appliance.

Examples

```
cli> s<Tab><Tab>
set   shell   show
cli> se<Tab>
cli> set
cli> set n<Tab><Tab>
network  ntp
cli> set ne<Tab>
cli> set network
cli> set network <Tab><Tab>
hostname hosts interface resolv  st_routes
cli> set network i<Tab>
cli> set network interface
cli> set network interface eth0 <Tab>
 address alias  gateway method mtu netmask
address6 broadcast gateway6 method6 mtu6 netmask6
```

CLI Commands

The CLI utility supports the commands that are described in the following sections with examples.

```
cli> <Tab><Tab>
add       commit    exit      list      rename    set       show
cd        delete    get       quit      revert    shell     version
```

add

The **add** command adds the last parameter and sets it to the default value (if any). Any nondefault values must be set using the **set** command.

The **add** command is used instead of **set** when multiple parameters of the same type can exist. For example, add network hosts <IP address> makes an entry for a host with the specified IP address in the hosts list. In that case, add is used because multiple hosts can exist.

In contrast, the **set** command (as in: set network interface eth0 address <IPaddress>) is used to specify the IP address for the eth0 Ethernet interface. In that case, the **set** command is used because each interface has only one IP address.

Adding certain parameters causes one or more related parameters to be added to the subtree. For example, when an IP address is added to the hosts list, empty hostname and alias parameters are also added. For some parameters, a set of meaningful default values are assigned. For empty parameters, the **get** or **show** commands list the parameter names without any values.

You must add parameters in a prescribed order. For example, because an empty hostname and alias parameters are created when you add a host's IP address, you cannot add a host by name before specifying the host's IP address, and you cannot specify the host name at the same time as its IP address. To specify a name or alias for a host you need to add the host first by adding its IP address, then you need to use the **set** command to specify its name and alias.

Synopsis

```
add parameter(s) value(s)
```

Examples

```
cli> set network hosts 192.168.160.11 name fruitbat
'name' doesn't make sense in its context.
[set network hosts 192.168.160.11 name fruitbat] Failed: Invalid input
cli> get network hosts 192.168.160.11 name
Words 4 and following were ignored.
cli> add network hosts 192.168.160.11
OK
cli> get network hosts 192.168.160.11
network hosts 192.168.160.11 name
network hosts 192.168.160.11 alias
cli> set network hosts 192.168.160.11 name fruitbat alias fbat
OK
cli> get network hosts 192.168.160.11
network hosts 192.168.160.11 name: fruitbat
network hosts 192.168.160.11 alias: fbat
```

Parameters that can be added

The following table shows the parameters that can be added using the **add** command. Table 6.3 on page 112 shows additional parameters and values that must be set for each parameter after the parameter is added. When a parameter is shown in the Parameter Level 2 column, the Parameter Level 1 and Parameter Level 2 parameters must be entered together with the **add** command; for

example, to add a service processor user, you must enter **add spmanager user <username>**; the user must then be configured after adding, using the **set** command.

Table 6.2: Parameters that Work with the CLI add Command

Parameter Level 1	Parameter Level 2	What It Configures (Syntax)
dhcpd	mapping	Add a MAC address for IP. **Synopsis:** add adhpd mapping <MAC_address> **Example:** add dhcpd mapping 00602e01d9a6 **NOTE:** No colon (:) is needed in the MAC address.
iptables	nat | filter	Firewall configuration. Add a new rule to NAT table and filter table. **Synopsis:** add iptables nat [PREROUTING|POSTROUTING|OUTPUT] <number>| filter [INPUT|OUTPUT|FORWARD] <chainname> **Example:** add iptables nat PREROUTING 0
network	interface	Add an alias to an interface. **Synopsis:** add network interface <interface> alias <alias_name> **Example:** add network interface eth1 alias yd
	hosts	Add an IP address for a host. **Synopsis:** add network hosts <IPaddress> **Example:** add network hosts 172.26.25.178
	st_routes	Add to the list of static route targets a subnet or host (networks in the form 1.2.3.0/24 or host IPs). **Synopsis:** add network st_routes <network_IPaddress/netmask> | <host_IPaddress> **Example:** add network st_routes 1.1.1.1
pxe	mapping	Add a MAC address. **Synopsis:** add pxe mapping <MAC_ address> **Example:** add pxe mapping 00602e01d9a6 **NOTE:** No colon (:) is needed in the MAC address.
snmpd	user	Add a user and fills in the subtree with default values and randomly generated passwords. **Synopsis:** add snmpd user <user_name> **Example:** add snmpd user user1
	group	Add a group. **Synopsis:** add snmpd group <group_name> **Example:** add snmpd group g1
	view	Add a view. **Synopsis:** add snmpd view <view_name> **Example:** add snmpd view ies

Table 6.2: Parameters that Work with the CLI add Command (Continued)

Parameter Level 1	Parameter Level 2	What It Configures (Syntax)
	access	Add an access type. **Synopsis:** add snmpd access <noauth|auth|authpriv> **Example:** add snmpd access auth
	com2sec	Add a com2sec type. **Synopsis:** add snmpd com2sec <type> **Example:** add snmpd com2sec mp1
	proxy	Add an snmpd proxy. **Synopsis:** add snmpd proxy <proxy_name> **Example:** add snmpd proxy 0
syslog	destination	Add the name of syslog server to the default console or rootuser destinations defined for syslog messages. **Synopsis:** add syslog destination <server_name> **Example:** add syslog destination dest1
spmanager	server	Two steps are required to add a server to the appliance: 1) Add a managed device to the appliance. **Synopsis:** add spmanager server <device_name> 2) Configure the device parameters for the appliance. **Synopsis:** set spmanager server <devicename> account_verify <yes|no> type <typename> ip <IP address> user <username> password <password> group <group name> **Example:** add spmanager server 172.26.25.236 set spmanager server 172.26.25.236 account_verify no type IBMBC ip 172.26.25.236 user USERID password PASSWORD group MergePoint **NOTE:** The group means the server group. The default group is MergePoint. To specify an alias or sol port to the server, see the spmanager server parameter in Table 6.3.
	user	Add the name of a user authorized to access the appliance. **Synopsis:** add spmanager user <username> **Example:** add spmanager user user11 **NOTE:** To set a device or a role to the user, see the spmanager user parameter in Table 6.3.

Table 6.2: Parameters that Work with the CLI add Command (Continued)

Parameter Level 1	Parameter Level 2	What It Configures (Syntax)
	group	Add the name of a user group. **Synopsis:** add spmanager group <group_name> **Example:** add spmanager group g1 **NOTE:** To specify a device or a user to access the group, see the spmanager group parameter in Table 6.3.
	server-groups	Add the name of a server group. **Synopsis:** add spmanager server-groups <groups_name> **Example:** add spmanager server-groups MergePoint2. **NOTE:** To add a device into a server group, see the spmanager server parameter in Table 6.3.
	global role	Add an appliance user role. **Synopsis:** add spmanager global role <role_name> **Example:** add spmanager global role role_aa **NOTE:** To set the privilege of the global role, see the spmanager global role parameter in Table 6.3.

cd

The **cd** command sets a parameter prefix for subsequent commands. The prompt then changes to indicate the prefix. Entered by itself, cd returns to the top level.

Synopsis

```
cd [parameter(s)]
```

Examples

```
cli> cd network
network> get hostname
dingo
network> set hostname kookaburra
OK
network> cd interface eth0
network interface eth0> set <tab><tab>
address    alias      broadcast  gateway    method     mtu        netmask
network interface eth0> set address 192.168.160.10 netmask 255.255.255.0
OK
```

```
network interface eth0> cd ..
network interface> cd eth1
network interface eth1> set address 192.168.50.10
OK
network interface eth1> cd
cli>
```

commit

The **commit** command saves changes in configuration files and creates a compressed copy of the configuration files in a backup directory.

NOTE: If you make a change but do not commit it, the configuration files are not updated, and your changes will be lost after the next reboot.

Synopsis

```
commit
```

delete

The **delete** command deletes the last parameter in the command line. Deleting certain parameters deletes associated parameters. For instance, if an IP address is deleted from the host list, other parameters associated with a host (name, alias) are also deleted.

Synopsis

```
delete parameter(s)
```

Some parameters cannot be deleted. Parameters that can be added can be deleted.

Examples

```
cli> get network hosts 192.168.160.11
network hosts 192.168.160.11 name: fruitbat
network hosts 192.168.160.11 alias: fbat
cli> delete network hosts 192.168.160.11
OK
cli> set network hosts 192.168.160.11 name fruitbat
'name' doesn't make sense in its contest.
[set network hosts 192.168.160.11 name fruitbat] Failed: Invalid input
cli> get network hosts 192.168.160.11 alias: fbat
Words 4 and following were ignored.
```

get | show

The **get** command retrieves the value assigned to a parameter. When no parameters are listed, the whole parameter tree is displayed. If full parameters are specified, the assigned value is displayed.

Synopsis

```
get | show parameter(s)
```

Examples

```
cli> get network hostname
anchovy
cli> show network resolv domain
avocent.com
```

When get is entered with a partial parameter, all the subtrees display. In the output, if a value is assigned, the parameter preceding the value ends with a semicolon.

```
cli> get network
network interface failover: no
network interface eth0 method: dhcp
...
network hosts 127.0.0.1 name: MergePoint
network hosts 127.0.0.1 alias: localhost
network st_routes
cli>
```

If the system assigns default values, default values are shown next to the automatically added parameter name, as in the following example, which was entered on the MergePoint SP manager before any configuration has been done.

```
cli> get network interface eth0
network interface eth0 method: dhcp
network interface eth0 address: 192.168.160.10
...
network interface eth0 gateway: none
network interface eth0 mtu: 1500
network interface eth0 alias
cli>
```

NOTE: If you make a change but do not commit it (see *commit* on page 107), the configuration files are not updated. The **get** command shows the changes that are currently stored in the RAM memory, not the actual value stored in the affected configuration file.

list

The **list** command lists all available parameters. With no parameters listed, the whole parameter tree is displayed. If parameters are specified, the corresponding subtree is displayed.

Synopsis

```
list parameter(s)
```

Example

```
cli> list network hosts
127.0.0.1
127.0.0.1 name
127.0.0.1 alias
192.168.160.10
192.168.160.10 name
192.168.160.10 alias
```

quit | exit

The **quit** command closes the CLI utility. (**Ctrl+d** also quits the CLI utility.) If changes have not been committed, the user is prompted to commit the changes or quit without committing.

Synopsis

```
quit
```

Example

```
cli> set network hostname frutabaga
OK
cli> quit
You have made changes but haven't committed them yet.
To commit the changes, use the "commit" command.
To revert all changes and quit without committing, use "quit!".
cli> commit
cli> quit
```

quit!

The **quit** command closes the CLI utility and discards any uncommitted changes.

rename

The **rename** command renames parameter. Depending on the parameter, this may result in a whole subtree of parameters being moved. For instance, if an IP address in the host list is changed, all parameters associated with that host (name, alias) are moved under the new name.

Synopsis

```
rename parameter(s) value(s)
```

Examples

```
cli> get network hosts 192.168.160.11
network hosts 192.168.160.11 name: fruitbat
alias
cli> rename network hosts 192.168.160.11 192.168.160.222
OK
cli> get network hosts 192.168.160.11
ERR No such file or directory
cli> get network hosts 192.168.160.222
name fruitbat
alias
```

revert

The **revert** command discards any changes and reverts to previously committed state.

Synopsis

```
revert
```

Examples

```
cli> get network hostname
dingo
cli> set network hostname kookaburra
OK
cli> get network hostname
kookaburra
cli> revert
OK
cli> get network hostname
dingo
```

set

The **set** command sets the value(s) of the last parameter. When multiple parameters are specified in one command, either all are set successfully or none of the values are changed.

The **set** command is used to set an existing value, in contrast to add command which is used to add something to the parameter tree. For example, this set command is used to specify the IP address for an Ethernet interface which already is identified by the eth0 parameter in the parameter tree: set network interface eth0 address <IPaddress>. In contrast, new hosts need to be added with the add command before their parameters can be specified; add network hosts <IPaddress> makes an entry for a host with the specified IP address in the hosts list. Parameters for this new host can then be changed with the set command: set network hosts <IPaddress> name <hostname>.

Synopsis

```
set parameter(s) value(s)
```

Examples

```
cli> set network resolv dns0 10.0.0.1
OK
cli> set network interface eth1 address 10.0.0.3 netmask  255.255.255.0
broadcast 10.0.0.255
OK
```

shell

The **shell** command escapes to the shell. This command is only available to root.

Synopsis

```
shell
```

Examples

```
cli> shell
root@MergePoint:~#
root@MergePoint:~# whoami
root
root@MergePoint:~# logout
cli>
```

version

The **version** command displays the current CLI version.

Synopsis

```
version
```

Examples

```
cli> version
MergePoint CLI 2.0 (2007-06-16T13:47+1000)
```

Summary of How to Configure the Top Level Parameters

This section provides a brief overview of how to configure the top level parameters.

Table 6.3 describes which of the top level parameters that you can set without using the **add** command first, and it also shows the parameters that need to be set after the **add** command creates the parameter to set additional parameters and values.

Table 6.3: Setting Top Level CLI Parameters

Parameter	Command
adsap2	Avocent DS Authentication Protocol configuration. **Synopsis:** set adsap2 state <secure | trust-all> authserver <ip-address> **Example:** set adsap2 state trust-all authserver 2.2.2.2 **NOTE:** The state of “secure” means the server is being managed by the DSView 3 software, while the state of “trust-all” means the server is unmanaged by the DSView 3 software. The parameter “authserver” specifies the IP address of authorization server.
auth	Use the **set** command with the *type* parameters to set an authentication type for logins to the MergePoint SP manager, either krb5, ldap, nis, radius, smb, or tacplus. Use the **set** command with the auth type ppp parameters to set an authentication type for logins through the auxport modem and pcmcia/cardbus modems. Authentication types supported for the MergePoint SP manager and for target devices are listed in *Configuring Authentication Services* on page 71. **Synopsis:** set auth type <typename> nis domainname <name> server <ip|broadcast> radius|tacplus accthost <server-name> authhost <server-name> secret <secret> timeout <count> retries <count> tacplus service <ppp|raccess> krb5 realm <realm> server <ip-address> ldap host <host> base <base-name> binddn <dn> bindpw <password> pam_login_attribute <attribute> ssl <on|off|start_tls> smb domain <name> server <ip-address> **Example:** set type local nis domainname subavt server 1.1.1.1 radius authhost1 a1 authhost2 a2 accthost1 c1 accthost2 c2 secret pwd timeout 4 retries 2 tacplus authhost1 1.1.1.1 authhost2 12.2.2.2 accthost1 1.1.1.1 accthost2 12.2.2.2 secret pwdd retries 2 timeout 4 service ppp krb5 realm dm server 2.2.2.2 ldap host 127.0.0.1 base dc=padl,dc=com binddn bdl bindpw pwd pam_login_attribute df ssl on smb domain sudom server1 2.2.2.1 server2 3.3.3.3

Table 6.3: Setting Top Level CLI Parameters (Continued)

Parameter	Command
bootconf	Use the **set** command to configure boot configuration. **Synopsis:** set bootconf wdt <yes|no> mac <mac address> ip <ip address> bootfile <file name> serverip <tftp server ip> baudrate <1200|2400|4800|9600|19200|38400|57600|115200> fecmode1|fecmode2 <auto|100F|100H|100F|10F|10H> BF_curr < 0| 1 |2> **Example:** set bootconf wdt yes mac 00:60:2e:01:d9:a6 ip 172.26.25.177 bootfile uImage.4.0.0.28 baudrate 9600 fecmode1 auto fecmode2 auto BF_curr 1 **NOTE:** This parameter is only for the MergePoint 5224/5240 appliance.
dhcpd setting subnet	Use the **set** command to configure dhcpd settings. **Synopsis:** set dhcpd setting subnet <subnet name> range_low <start ip> range_high <end ip> **Example:** set dhcpd setting subnet 199 range_low 199.1.1.1 range_high 199.1.1.160
dhcpd setting relay	Use the **set** command to specify a DHCP relay server. **Synopsis:** dhcpd setting relay server <relay server> status <yes/no> **Example:** set dhcpd setting relay server 172.26.25.3 status yes
dhcpd mapping	Use the **set** command to specify an IP address for added MAC. **Synopsis:** set dhcpd mapping <MAC_address> ip <ip_address> **Example:** set dhcpd mapping 00602e01d9a6 ip 1.1.1.1 **NOTE:** See the dhcpd parameter in Table 6.2.
iptables [filter | nat]	By default, a set of chains is defined with hidden rules. For NAT, the predefined chains are: PREROUTING, POSTROUTING, OUTPUT. For filter, the predefined chains are: INPUT, OUTPUT, FORWARD. For background information, see *Firewall/Packet Filtering* on page 18. Use the **set** command to configure a rule for a predefined chain after the **add** command is used to add a rule for that chain. Or use the **set** command to configure a rule after the **add** command is used to add a new chain and to add a new rule for the new chain (set iptables) <filter | nat> **<Tab> <Tab>** shows the current chains; set iptables <filter | nat> <chainname> shows the rules for a specific chain, and get iptables <filter | nat> <chainname> <rule_number> shows the configuration parameters to set filtering policies. **Synopsis:** set iptables nat PREROUTING|POSTROUTING|OUTPUT <number> | filter INPUT| FORWARD|OUTPUT <number> destination <ip> inv <yes|no> source <ip> inv <yes|no> protocol <pro> inv <yes|no> dport <port> inv<yes|no> sport <port> inv<yes|no> in-interface <in> inv<yes|no> out-interface <out> inv<yes|no> fragment <head|nonhead|all> target <rule> to-source <ip> to-destination <ip> **Example:** set iptables nat PREROUTING 0 destination 127.2.2.2 inv yes source 127.2.2.1 inv yes protocol tcp inv no dport 9000 inv no in-interface eth0 inv no fragment head
network hostname	Use the **set** command to configure the hostname for the MergePoint SP manager. **Synopsis:** set network hostname <hostname> **Example:** set network hostname MergePoint1 **NOTE:** By default the hostname is MergePoint.

Table 6.3: Setting Top Level CLI Parameters (Continued)

Parameter	Command
network hosts	After the **add** command is used to add a host to the hosts table, use the **set** command to configure the host's IP address and optional alias. **Synopsis:** set network hosts <IPaddress> name <host_name> alias <alias_name> **Example:** set network hosts 192.168..100 host MergePoint5200 alias MP5200 **NOTE:** See the network hosts parameter in Table 6.2.
network interface eth0|eth1 for IPv4	Use the **set** command to configure one of the network interfaces with IPv4 for the MergePoint 5200 appliance. **Synopsis:** set network interface eth0|eth1 method <static|dhcp> address <ip> netmask <netmask> broadcast <broadcast> gateway <ip> mtu <num> alias <alias name> **Example:** set network interface eth1 method static address 192.168.1.100 netmask 255.255.255.0 gateway 192.168.1.1
network interface bond0|eth0|eth1|priv0|br0 for IPv4	Use the **set** command to configure one of the network interfaces with IPv4 for the MergePoint 5224/5240 appliance. **Synopsis:** set network interface bond0|eth0|eth1|priv0|br0 method <static|dhcp> address <ip> netmask <netmask> broadcast <broadcast> gateway <ip> mtu <num> alias <alias name> **Example:** set network interface br0 method static address 192.168.1.100 netmask 255.255.255.0 gateway 192.168.1.1 set network interface priv0 address 192.168.1.120 netmask 255.255.255.0
network interface eth0|eth1 for IPv6	Use the **set** command to configure one of the network interfaces with IPv6 for the MergePoint 5200 appliance. **Synopsis:** set network interface eth0|eth1 method6 <dhcpv6|static> address6 <ip> netmask6 <netmask> gateway6 <ip> mtu6 <num> **Example:** set network interface eth1 method6 static set network interface eth1 address6 fe80:2001::2 netmask6 64
network interface bond0|eth0|eth1|priv0|br0 for IPv6	Use the **set** command to configure one of the network interfaces with IPv6 for the MergePoint 5224/5240 appliance. **Synopsis:** set network interface bond0|eth0|eth1|priv0|br0 method6 <dhcpv6|static> address6 <ip> netmask6 <netmask> gateway6 <ip> mtu6 <num> **Example:** set network interface bro method6 static set network interface br0 address6 fe80:2001::2 netmask6 64

Table 6.3: Setting Top Level CLI Parameters (Continued)

Parameter	Command
Note for IPv6	• Method6 has 2 valid value: dhcpv6, static. dhcpv6 - Interface gets its ipv6 address from dhcp server and other network settings from ipv6 RA or other valid information. static - You must set ipv6 address and other network settings manually. • Netmask6 is a number with value between 1 and 128. • IPv6 addresses are 16-byte numbers written in hexadecimal in blocks of 2-bytes separated by a colon. As an example: fdeb:8024:0000:0023:0000:0000:0a05:a0da. Leading zeros can be removed, changing our example into fdeb:8024:0:23:0:0:a05:a0da. One or more zeroed blocks can be substituted by a single "::", but only one such a substitution is allowed. This gives us two possibilities for our previous example: • fdeb:8024::23:0:0:a05:a0da • fdeb:8024:0:23::a05:a0da Note that fdeb:8024::23::a05:a0da is not allowed because it is ambiguous. Netmask6, also know as prefix length in IPv6 context, are usually encoded as the number of bits in prefix. • Mtu6 is a number with value between 1 and 1500.
network interface mode	Use the **set** command to specify a mode. **Synopsis:** set network interface mode normal|failover|bridge **Example:** set network interface mode bridge **NOTE:** This parameter is only for the MergePoint 5224/5240 appliance.
network resolv	Use the **set** command to configure DNS domain and one or more DNS servers. **Synopsis:** set network resolv dns0|dns1 <DNS_IP> domain <domain_name> **Example:** set network resolv dns0 172.26.24.3 dns1 172.20.1.11 domain corp.avo.com
network st_routes	After using the **add** command to add a static route to the routing table, use the **set** command to configure the static route. **Synopsis:** set network st_routes <ip> [gateway <ip>] [device <interface name>][metric <num>] **Example:** set network st_routes 1.1.1.1 device eth2 metric 0 **NOTE:** See the network st_routes parameter in Table 6.2.
ntp server	Use the **set ntp** command to specify an internet time server to sychronize. **Synopsis:** set ntp server <ip or hostname> **Example:** set ntp server clock.redhat.com
ntp enabled	Use the **set ntp** command to run the ntp server. **Synopsis:** set ntp enabled <yes|no> **Example:** set ntp enabled yes
pxe mapping	Use the **set** command to specify an IP address for added MAC. **Synopsis:** set pxe mapping <mac> ip <ip-address> **Example:** set pxe mapping 00602e01d9a6 ip 2.2.2.2 **NOTE:** See the pxe mapping parameter in Table 6.2.

Table 6.3: Setting Top Level CLI Parameters (Continued)

Parameter	Command
pxe setting	Use the **set** command to configure pxe settings. **Synopsis:** set pxe setting subnet <subnet> netmask <mask> gateway <gateway> sp_user <user name> sp_pwd <password> range_low <ip_address> range_high <ip_address> vlan_enable <yes|no> vlan_id <num> vlan_priority <num> **Example:** set pxe setting subnet 343 netmask 255.255.255.0 gateway 2.2.2.2 sp_user usr1 sp_pwd dff range_low 1.1.1.1 range_high 1.1.1.5 vlan_enable yes vlan_id 3 vlan_priority 2
snmpd access	After using the **add snmpd** command to add access, use the **set snmpd** command to configure the parameters. **Synopsis:** set snmpd access **Example:** set snmpd access **NOTE:** See the snmpd access parameter in Table 6.2.
snmpd com2sec	After using the **add snmpd** command to add com2sec, use the **set snmpd** command to configure the parameters. **Synopsis:** set snmpd com2sec<name> context <context> source <src> name <words> **Example:** set snmpd com2sec mp1 context contxt source 123.23.1.1 name mp **NOTE:** See the snmpd com2sec parameter in Table 6.2.
snmpd group	After using the **add snmpd** command to add group, use the **set snmpd** command to configure the parameters. **Synopsis:** set snmpd group <grp> sec_model <v1|v2c|usm> sec_name <name> **Example:** set snmpd group g1 sec_model v1 sec_name serc1 **NOTE:** See the snmpd group parameter in Table 6.2.
snmpd proxy	After using the **add snmpd** command to add proxy, use the **set snmpd** command to configure the parameters. **Synopsis:** set snmpd proxy <num> context <name> version <1|2c|3> community|user <name> oid <oid> sec_level <level> authmethod <MD5|SHA> authpass <pwd> privmethod <DES|AES> privpass <pwd> **Example:** set snmpd proxy 0 user user1 oid .1.1.1.1.1.10 sec_level 2 authmethod MD5 authpass 23545 privmethod DES privpass e4543 **NOTE:** See the snmpd proxy parameter in Table 6.2.
snmpd user	After using the **add snmpd** command to add user, use the **set snmpd** command to configure the parameters. **Synopsis:** set snmpd user <user> authmethod <SHA|MD5> authpass <pwd> cryptmethod <DES|AES> cryptpass <pwd> **Example:** set snmpd user user1 authmethod SHA authpass ert8Gftty cryptmethod DES cryptpass syOUSfda **NOTE:** See the snmpd user parameter in Table 6.2.

Table 6.3: Setting Top Level CLI Parameters (Continued)

Parameter	Command
snmpd view	After using the **add snmpd** command to add view, use the **set snmpd** command to configure the parameters. **Synopsis:** set snmpd view <name> <0|1|2|3|4|5> incl_excl <included|excluded> subtree <oid> mask <hex> **Example:** set snmpd view ies 0 incl_excl included mask ff subtree .1.1.1.1.1.0 **NOTE:** See the snmpd view parameter in Table 6.2.
snmpd syslocation|syscontact	Use the **set** command to specify the location of the system and the contact information. **Synopsis:** set snmpd syslocation <location name> syscontact <info> **Example:** set snmpd syslocation MergerPoint syscontact Avt
spmanager group	After using the **add** command to configure a user group, use the **set** command to configure the parameters. **Synopsis:** set spmanager group <name> user <name> target <target> **Example:** set spmanager group g1 user user1 target 172.26.25.39 **NOTE:** See the spmanager group parameter in Table 6.2.
spmanager server	After using the **add** command to configure a device, use the **set** command to configure the parameters such as account_verify, type, ip, group, alias, user, password or sol port. The account_verify “yes” indicates that the server is added with user account verification; while the account_verify “no”indicates that the server is added without user account verification. **Synopsis:** set spmanager server <devicename> account_verify <yes|no> ip <server_IP> group <server-group> alias <alias_name> user <username> password <pwd> sol_port <port> **Example:** set spmanager server 172.26.25.121 account_verify no type ilo ip 172.26.25.121 user root password admin sol_port 9500 set spmanager server 172.26.25.121 account_verify yes user root password admin **NOTE:** You can set an unverifed server to a verified server; but you cannot set a verified server to an unveified server. See the spmanager server parameter in Table 6.2.
spmanager user	After using the **add** spmanager user command to configure a user, use the **set** user command to configure the user’s parameters: role and target. **Synopsis:** set spmanager user <name> role <role name> target <target> **Example:** set spmanager user user11 role operator target 172.26.25.179 **NOTE:** The range of a role name is admin, operator, user and user defined role(s). To add a user role, see the add spmanager global role command in Table 6.2 on page 104. See the spmanager user parameter in Table 6.2.

Table 6.3: Setting Top Level CLI Parameters (Continued)

Parameter	Command
spmanager global role	After using the **add** spmanager global role command to add a user role, use the **set** command to configure the user role's privileges -the device management actions. **Synopsis:** set spmanager global role <name> privilege power <yes|no> coldest <yes|no> directcommand <yes|no> pxe <yes|no> snmp <yes|no> lan <yes|no> user <yes|no> alert <yes|no> sol <yes|no> bmctime <yes|no> sel <yes|no> sensor <yes|no> spconsole <yes|no> devconsole <yes|no> rdp <yes|no> **Example:** set spmanager global role role_aa privilege power yes pxe yes **NOTE:** See the spmanager global role parameter in Table 6.2.
sshd protocol	Use the **set sshd protocol** command to set the SSHD protocol version to either 1 or 2 or both (1,2 or 2,1). Default is 2,1. **Synopsis:** set sshd protocol <1|2|1,2|2,1> rootlogin <yes|no> port <num> **Example:** set sshd protocol 1 rootlogin no port 22 **NOTE:** Using this command is not recommended. Changed SSHD protocol version or SSHD port may cause some features from the web interface to fail.
syslog destination	Use the **set syslog destination** command parameters to configure a syslog destination (either the MergePoint SP manager console or rootuser or a syslog server name that has been added using the **add** syslog destination <syslog_server_name> command). **Synopsis:** set syslog [destination<dest> enable <yes|no> type <type> usertty <username> tcp <ip> udp <ip> file <file name> pipe <name> template <num> **Example:** set syslog destination dest1 enable yes type tcp tcp 127.2.2.2 **NOTE:** See the syslog destination parameter in Table 6.2.
syslog filter	Use the **set syslog filter** command to enable a syslog filter level. **Synopsis:** set syslog filter sysfilter|webfilter level <emerg|alert|crit|err|warn|notice|info|debug <yes | no> **Example:** set syslog filter sysfilter level emerg no alert no err yes notice yes
syslog presets	Use the **set syslog presets** command to set yes or no for enabling syslog to the root user or console. **Synopsis:** set syslog presets rootuser|console <yes|no> **Example:** set syslog presets rootuser yes console yes
timezone	Use the **set timezone** command to specify the timezone using a file relative to /etc/timezone.conf, for example GMT+8. **Synopsis:** set timezone <timezone> **Example:** set timezone GMT+5

Table 6.3: Setting Top Level CLI Parameters (Continued)

Parameter	Command
tcpdump source-ip|source-port|destination-ip|destination-port|protocol|interface	Use the **set tcpdump** command to define the IP packge filter parameters for the debug. **Synopsis:** set tcpdump source-ip <source_iP> source-port <source_port> destination-ip <destination_ip> destination-port <destination_IP> protocol <all|ip|tcp|udp|icmp|igmp> interface <interface> **Example:** set tcpdump source-ip 1.1.1.1 source-port 1500 destination-ip 1.1.1.49 destination-port 1500 protocol ip interface eth0 **NOTE:** For the MergePoint 5200 appliance, the interface is all, eth0 or eth1. For the MergePoint 5224/5240 appliance, the interface is all, eth0, eth1, priv0, bond0 or br0.
tcpdump state	Use the **set tcpdump** command to start or stop the debug. **Synopsis:** set tcpdump state on|off **Example:** set tcpdump state on **NOTE:** Setting the state to on or off will start or stop the tracing process.

APPENDICES

Appendix A: Troubleshooting

Port mapping fails when using DirectCommand

This section describes some considerations that may apply if port mapping fails when a user attempts DirectCommand access to a target device.

If DirectCommand is invoked by an unprivileged user (such as a regular user on a UNIXbased system), DirectCommand may not be able to open privileged TCP ports (numbered below 1024). DirectCommand attempts to open the port by adding an offset to any requested port number that is less than 1024 and by automatically modifying the URL to represent the new local port. However, if the service provided by a target device can operate only on the original predetermined TCP port, DirectConnect does not work properly and displays a descriptive warning. If this occurs, DirectConnect connections may be made to the target device only by workstation administrators.

Another possible cause for failed port mapping by Direct Command is that the user's workstation may be running an application that uses a TCP port that is needed by DirectCommand. For example, if the user's workstation is running a web server on port 80 and the target device being accessed through DirectCommand expects port 80 to be mapped, DirectCommand might not work. To prevent this kind of conflict, make sure that local applications running on the user's workstation do not use the same TCP port numbers used by DirectCommand.

Login failure

If no one can log into the MergePoint 5224/5240 appliance, you can perform the following procedure to reset the root or admin user's password. This procedure would be needed, for example, if an attempt to log into the console as root brings up the following message:

```
login[212]: FAILED LOGIN
1 FROM  FOR root, User not known to the underlying
authentication module
Login incorrect
```

To recover from login failure:

1. Make a terminal connection to the MergePoint 5224/5240 appliance.
2. Turn power off and then on to physically reboot the MergePoint 5224/5240 appliance.
3. When prompted, hit any key to interrupt the boot and enter UBoot monitor mode.

   The UBoot monitor prompt appears as shown in the following example.

   ```
   root@MergePoint:~# reboot
   ...
   Hit any key to stop autoboot: 0
   ```

```
=>
```

4. Boot in singleuser mode:

```
=> setenv bootargs $bootargs single
=> boot
```

5. When single user mode comes up, use the passwd command to change the root or admin user's password. The following example shows changing the admin user's password.

```
bash-3.00# passwd admin
Enter new UNIX password: admin_password
Retype new UNIX password: admin_password
Passwd(pam_Unix)[2130]: password changed for admin
bash-3.00#
```

6. Restart the MergePoint SP manager to return to multiuser mode.

```
bash-3.00# reboot
```

   The root or admin user should now be able to log in with the new password.

7. Reconfigure authentication as desired.

Firmware image is corrupted

Information in Boot file location gives an administrator who knows the root password enough background to be able to boot from an alternate image if the need arises and if the web interface is not available.

Network boots are recommended for troubleshooting only. For example, if you want to test a new release of the firmware to make sure a problem is fixed, or if the removable Flash memory becomes corrupted, you could download the firmware to a tftpboot server and boot the appliance with it. After you test the image or replace the damaged Flash, if needed, you can then save the firmware image to the removable Flash using the **create_cf** command.

You can use the **create_cf** command when troubleshooting problems with the boot image, as described under *To upgrade to a boot image from a network boot:* on page 144.

Resetting the MergePoint 5200 appliance

If necessary, you can use the following options to reset the MergePoint 5200 appliance.

To reset the MergePoint 5200 appliance through a serial connection:

1. Connect a terminal or a workstation that is running a terminal emulation program to the serial port.
2. Start a session with the port settings of serial speed as 9600 bps, data length as 8 data bits, parity as none, stop bits as 1, flow control as none and emulation as ANSI.

   Once a connection is established, a prompt appears.

3. To restart the appliance, type **5** (Reboot).

   -or-

To reset the appliance network settings and remove licenses, type **5** (Reboot) and press **Ctrl + Z** when prompted to enter the next menu. All appliance settings will be erased.

-or-

To remove all target devices, type **10** (Restore to Factory Default). All target device IP addresses are erased, but the appliance network settings and licenses remain intact.

-or-

To reset the MergePoint SP manager to a previous firmware version, type **7** (Roll back the version). Type **0** (Exit) to exit.

Appendix B: Technical Specifications

Table B.1: MergePoint 5200 Appliance Technical Specifications

Network Connection	
Number	2
Type	Ethernet, 10BaseT, 100BaseT, GigE
Connector	RJ-45
Serial Port	
Number	1
Type	RS-232 serial
Connector	DB9 male
Mechanical	
H x W x D	4.3 x 42.7 x 35.6 cm (1.7 x 16.8 x 14 in), 1 U form factor
Weight	5.9 kg (13 lb)
Power	
AC Input Voltage	100 to 240 VAC
Rated Input Current	4A maximum
Rated Input Frequency	50 to 60 Hz
Rated Output Power	260 W maximum
Rated Output Voltages	+3.3 V (15 A), +5 V (25 A), +12V (18A), -12 V (1A)
BTU Rate	1400 Bus/hour (for rated output power of 260 W)
Environmental	
Temperature	0° to 35° Celsius (32° to 95° Fahrenheit) operating
Humidity	10 to 90% noncondensing operating
Safety and EMC Approvals and Markings	USA (UL, FCC), Canada (cUL), Germany (TUV), European Union (CE), Japan (VCCI), Russia (GOST) and Korea (MIC)
NOTE: Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.	

Table B.2: MergePoint 5224/5240 Appliance Specifications

Hardware	
CPU	Freescale Power QUICC III
Memory	256 MB DDRAM/128 MB compact Flash
Interfaces	24/40 Ethernet 10/100 BT on RJ45
	1 RS232 console on RJ45
	1 RS232 DTE on RJ45 for power manager or external modem
	1 10/100/10000 BT Ethernet on RJ45 (primary)
	1 10/100 BT Ethernet on RJ45 (optional secondary or failover)
Dual 32/16 bit PCMCIA Slots:	Supported PC card types listed at www.avocent.com
Enclosure	1U Steel
Dimensions (WxDxH)	43.18 x 80 x 4.45 cm (17 x 12 x 1.75 in)
Environmental	
Operating Temperature	10° to 50° Celsius (50° to 122° Farenheit)
Storage Temperature	40° to 85° Celsius (40° to 185° Farenheit)
Humidity	5% to 90% noncondensing
Electrical	
Power	Universal AC: single or dual 100240 VAC, 50/60Hz, 1.4 A max Dual DC: 36 to 75 VDC, 5 A max
Safety and EMC Approvals and Markings	CSA, FCC, C-tick, Japan (VCCI), European Union (CE)

NOTE: Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.

NOTE: To comply with FCC and CE certification requirements, use shielded cables when connecting target devices to Ethernet ports. Failure to observe these requirements makes the equipment no longer compliant.

Appendix C: Access Privileges

This appendix shows the access privileges that are required when the listed actions are performed either by appliance users or target device users. To set privileges for a MergePoint SP manager user, see *Managing MergePoint SP manager user accounts* on page 22. To set privileges for a target device user, see *Managing user accounts on target devices* on page 33.

Appliance users actions

NOTE: Admin users can perform all actions on appliances and target devices.

The following appliance user actions can be performed by Operators:

- To power a target device up/down
- To set LED indicator on/off for a target device
- To set target device cold reset
- To execute a self test
- To power a device group up/down
- To edit the target device user (including enable user, username, password and privilege)
- To set the event alert destination (PET) setting for a target device
- To set the event destination (PET) setting for a group
- To edit the SoL configuration
- To set the target device time for a target device
- To clear all SEL records

The following appliance user actions can be performed by all users:

- To view the alert actions list
- To query alerts
- To log in/out of the appliance
- To show the appliance version on the interface
- To show the Help document
- To view the summary of license information
- To view target device system name
- To view target device firmware information
- To view target device FRU information
- To view target device power status
- To view chassis status
- To view LAN configuration
- To view target device user information (except password)
- To view the event alert destination (PET) setting

- To view the SoL configuration
- To view the current target device time
- To view SEL records
- To view sensors information
- To view SoL summary
- To execute SoL
- To view SoL history
- To execute SoL relay
- To view SEL records
- To view sensors information
- To view SoL summary
- To set target device RDP for a target device
- To set VNC for a target device

Target device users

The following target device user actions can be performed by all Operators:

- To view/edit LAN configuration
- To view target device user information (except password)
- To edit the target device user (including enable user, username, password and privilege)
- To view the event alert destination (PET) setting
- To set the event alert destination (PET) setting for a target device
- To set the event destination (PET) setting for a group

The following target device user actions can be performed by all users:

- To view target device system name
- To change alias for a target device
- To copy/move a target device to a device group
- To remove a target device
- To view target device firmware information
- To view target device FRU information
- To view target device power status
- To power a target device up/down
- To view chassis status
- To set LED indicator on/off for a target device
- To set target device cold reset
- To execute a self test

- To power a device group up/down
- To view the SoL configuration
- To view the current target device time
- To view SEL records
- To view sensors information
- To view SoL summary
- To execute SoL
- To view SoL history
- To execute SoL relay
- To view SEL records
- To view sensors information
- To view SoL summary
- To set target device RDP for a target device
- To set VNC for a target device

Appendix D: Configuring the BIOS Settings for SoL

SoL enables the console output of a managed system to be redirected over an IPMI session over IP. This allows remote users to have text-based access to the BIOS, utilities, operating systems such as Command Line interfaces and Linux console and management services such as Microsoft's serial-based EMS. At the same time, SoL provides access to IPMI platform management functions.

To set the BIOS:

1. Enter the BIOS setting.
2. Select the *Console Redirection* option.
3. Point to Console Redirection and press **Enter**.
4. Change the Redirection After Boot value from Disabled to Enabled.
5. Save the settings to BIOS.

To set the BIOS with Windows 2003:

If your operating system is Windows 2003 Enterprise, enter the following command in the command line:

```
bootcfg /ems ON /port com1 /baud 19200 /id 1
```

To set the BIOS with Redhat Enterprise Linux 3.0:

1. Modify the /etc/grub.conf

```
#serial -unit=0 -speed=19200
#terminal -timeout=10 serial console
default=10
timeout=10
#splashimage …
Title Red Hat Linux …
    root (hd0,2)
    kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6
console=tty1 console=ttyS0,19200
    initrd-2.4.18-4smp.img
```

2. Modify the /etc/inittab by adding the following text to the end:

```
7:2345:respawn:/sbin/agetty -h ttyS0 19200 vt100
```

3. Modify the /etc/securetty by adding the following text:

```
ttyS1
```

Appendix E: Configuring a Virtual Serial Port

The MergePoint SP manager has the ability to access target devices with iLO through the Virtual Serial port. To use this feature, you must enable the Virtual Serial port on both the BIOS Serial Console and EMS Console. When the Virtual Serial port is enabled, it provides remote access through the iLO management controller to the BIOS Serial Console.

To configure BIOS Serial Console:

1. Enter ROM-Based Setup Utility by pressing **F9** during power up or system reset.
2. Select *BIOS Serial Console and EMS* on the main menu and press **Enter** to display the options.
3. Select *BIOS Serial Console Port*, then press **Enter** to display the options.
4. Select *Com1* or *Com2* as the BIOS Serial Console Port and press **Enter** to save the selection.

To configure EMS Console:

1. Enter ROM-Based Setup Utility by pressing **F9** during power up or system reset.
2. Select *BIOS Serial Console and EMS* on the main menu and press **Enter** to display the options.
3. Select *EMS Console*, then press **Enter** to display the options.
4. Select the same port that you selected for the BIOS Serial Console Port and press **Enter** to save the selection.

Appendix F: Profile Configuration

The MergePoint SP manager uses profiles for handling communications with target devices. Profiles are introduced in *Managing SP Profiles (Admin users only)* on page 31. Administrator-modifiable parameters that are defined for each profile are Family and Command Template, either or both of which can be modified to enable communications with target devices that do not work out of the box.

Families, Expect scripts and command templates

Each target device should belong to a family. Each target device family is defined by an Expect script in the /etc/libexec/mergepoint directory in the form: talk_<family_name>.exp. For example, the Expect script that defines the iLO family is talk_ilo.exp.

The Expect scripts use text-based interfaces that are in command templates to log into the target devices and perform supported management actions on behalf of authorized users. One Expect script and one command template are assigned to each target device.

Because the default Expect scripts and command templates do not always work for all types of target devices, or for all target devices of the same type, you need to create a custom family (Except script), or create / modify a command templates as desired.

For a new target device type, you need to perform the following procedures:

- Create a custom family (Except script)
- Create a user profile
- Test the existing template with the selected family
- If the test is failed, then create new or modify a command template

For a target device of an existing type, but using different commands, you need to perform the following procedures:

- Create a user profile
- Test the existing template with the selected family
- If the test if failed, then create new or modify a command template

Creating custom families

To create a new device family, the administrator can create a customized Expect script by copying, renaming and modifying one of the default Expect scripts. The administrator should set the file permissions to allow reading and execution by all users and writing by members of the admin group. The format of a custom Expect script's file name should be: talk_customN.exp.

NOTE: Administrators need to create new Expect scripts for new families by using talk_custom1.exp, talk_custom2.exp, or talk_custom3.exp for the filenames in the /etc/libexec/mergepoint directory.

To create a custom family (Expect script):

1. Log into the MergePoint SP manager console as **admin**.

2. Go to the /etc/libexec/mergepoint directory.
3. A user can create a new script talk_customN.exp or copy an existing talk_<family_name>.exp and name the new file in the format: talk_customN.exp.

NOTE: Use *talk_custom1.exp* for the first custom script, *talk_custom2.exp* for a second, up to a total of three scripts.

4. Edit the script as desired.
5. Save and quit the file.
6. Make sure the permissions are still 755.

NOTE: Contact your Avocent representative if you need additional support for creating a custom Expect script.

Default family names and corresponding Expect script names

Table F.1: Default Family Names and Corresponding Expect Script Names

Family Name	Expect Script Name
alom	talk_alom.exp
blade_center	talk_blade_center.exp
iLO	talk_ilo.exp
rsa_II	talk_rsa_II.exp
drac	talk_drac.exp
devconsole	talk_devconsole.exp
ilom	talk_ilom.exp
drac_mc	talk_drac_mc.exp
hp_blade_system	talk_hp_blade_system.exp
custom1	talk_custom1.exp
custom2	talk_custom2.exp
custom3	talk_custom3.exp

NOTE: There are no corresponding Expect script files to families "dell_10g", "ipmi_1.5", "ipmi_2.0" and “fsc_irmc”.

Service processor/device Expect script arguments

With one exception, each of the Expect scripts used to control access to a service processor takes exactly five arguments in the following format:

```
talk_type.exp ip user passwd spprofilename action
```

The exception to the format above occurs when the action is spconsole. When the fifth argument is spconsole, any other number of arguments may follow; all arguments entered after the spconsole actions are collected into a single command to be executed in the target device's native command interface.

```
talk_type.exp ip user passwd spprofilename spconsole
[command1|...|commandN]
```

ip, user, passwd, spprofilename

These four arguments separately represent the IP address, username, password or profile name of the device on the MergePoint SP manager.

action

The action specifies the action for the script to take. The actions are listed below. Not all device types implement all of the listed actions. For example, the iLO type does not have a sensors reading feature, so the sensors action is not supported for iLO type servers. See *Service processor/device Expect script exit codes* on page 133 for the correct way to handle an unexpected action argument.

- Sensors: Asks the service processor for a sensor reading and displays service processor sensor output on standard output.
- poweron: Asks the service processor to turn on its server.
- poweroff: Asks the service processor to turn off its server.
- powercycle: Asks the service processor to reboot its server.
- powerstatus: Asks the service processor if its server is turned on.
- reset: Asks the service processor to reset its server.
- spconsole: The native command line of the service processor. Enters interactive passthrough mode. The script authenticates with the service processor, then connects the output directly to its standard output and its standard input to the input.

NOTE: SSH must be invoked with the -t option when this mode is used.

- devconsole: Enters a console (also known as device console) session on a server whose service processor supports console access to the server or enters a console session on a server or other device that supports device console access through its Ethernet port.

NOTE: SSH must be invoked with the-t option when this mode is used.

Service processor/device Expect script exit codes

Scripts that handle devices must end with one of the exit codes shown in Table F.2.

Table F.2: Expect Script Exit Codes

Exit Code	Definition
0	Success

Table F.2: Expect Script Exit Codes

Exit Code	Definition
1	Unexpected output from service processor/device, or another error in an protocol (such as time-out)
3	Failed to connect with service processor
4	Host identification failed (only for connection through SSH)
5	User verification failed
6	Command template not found
7	Some necessary information not found in command template
10	Invalid argument
11	Action not supported

Creating a profile

Profiles are introduced in *Managing SP Profiles (Admin users only)* on page 31.

Configuring command templates

When adding a new target device that needs a template, the administrator must perform the following actions:

- Test whether the target device is compatible with the applicable default command template.
- If communications cannot be established with the new target device using a default command template, use the sptemplate utility to create and test a new command template, after making any needed changes to the commands that manage communications between the target device and the MergePoint SP manager.
- If a new template cannot be made to work, create a custom Expect script to handle the target device's requirements.

When one of the command templates is modified by an administrator, it applies to all target devices that use the template. Create a new template using the Web interface when you do not wish to overwrite one of the defaults.

To find out if an existing command template works with a new target device:

1. Assign the target device the appropriate profile and the associated default command template for the profile.
2. Try to run power management commands on the target device.
3. If you can run power commands on the target device, test the rest of the management commands that are supported on the device type. If they work, you are done.

4. If you cannot run one or more of the supported commands on the target device, attempt to connect to the console.

NOTE: Even if the power management commands do not work on a new target device, you can usually establish a connection to the service processor's console.

5. If you cannot access the console, perform the following steps:
   a. Use ping, Telnet or SSH to verify that you can get to the server.
   b. If you cannot access the server, check the network configuration and fix the problem that is preventing access.
6. If you can access the server but still cannot access the service processor's console, double-check the username and password you are using against the username and password that are configured for the target device.
7. Once you have established the connection to the service processor's console, type the help command, which gives you the syntax you need to use for the commands supported by the service processor.
8. Note the syntax of the commands supported by the service processor's console, and go to the next procedure.

To use the sptemplate utility to create a new template:

Perform this procedure after *To find out if an existing command template works with a new target device:* on page 134 if the default templates do not work for a new target device.

NOTE: If you select *Profile* in the Web interface and select the *Templates configuration* button, you are logged into the console and the sptemplate utility automatically launches. Go directly to step 2.

1. Log into the console as an administrator.
2. Select *New* from the menu.
3. Enter a name, such as rsa.new. The editor brings up a template for a new command template and assigns it the name you specified. See *Using the sptemplate utility* on page 137 for details.
4. Modify the prompts and commands as needed, using the syntax supported on the target device. Sensors may not be supported. If any command is not supported, leave it commented out in the template.

NOTE: You must specify the escape sequence used by the device's console. It is captured by the MergePoint SP manager and it is used to log the user out of the SP console whenever the user logs out of the device console, preventing unauthorized access to the SP console.

5. Save and quit the file.
6. Enter the **saveconf** command.
7. Log out from the console.
8. Log in to the Web interface as an administrative user and select *Target - Profile*.
9. In the User Profile area, click *Add*.

10. In the Command Template drop-down menu, the new template is automatically added and is included in the list of command templates that you can assign to a profile.
11. Assign the new template to the profile.

NOTE: The new template is automatically added to the Command Template drop-down menu the next time an administrative user logs into the web interface.

To use the sptemplate utility to test a template:

When sptemplate is used to test a template, extra debugging information is provided to report on commands sent to and received from the target device.

1. Log into the console as an administrator.
2. Select *Test* from the menu.
3. At the prompt, confirm that you want to continue by entering **y**. A list of templates appears.
4. Select a template to test. A list of configured target devices appears.
5. Select a target device to test the template against. The editor runs the commands in the specified template and returns debugging information that you can record for making command changes in a new template.
6. Choose a command to test.
7. At the prompt, enter the username and password you used when logging into the MergePoint SP manager.
8. Go to *To use the sptemplate utility to create a new template:*.

Default command templates

Default Command Templates lists the default command templates and describes the types of target devices to which they apply.

Table F.3: Default Command Templates

Template	Type of Target Device
alom.default	Sun ALOM type target devices
blade_center.default	IBM BladeCenter type target devices.
devconsole.default	Target devices that support access to their consoles.
drac_mc.default	Dell DRAC MC target devices.
drac3.default	DRAC III type target devices.
drac4.default	DRAC IV type target devices.
drac5.default	DRAC V type target devices.
hp_blade_system.default	HP BladeCenter target devices.

Table F.3: Default Command Templates (Continued)

Template	Type of Target Device
hp_ipmi.default	HP IPMI target devices.
ilo.default	iLO type target devices.
ilom.default	ILOM type target devices.
None	• IPMI 1.5 type target devices. • Any type target device when only native IP access is being configured.
rsa.default	Standard RSA II type target devices.
rsa_withoutsol.default	RSA II type target devices do not support SoL.

NOTE: You cannot change templates whose name ends with the .default suffix. sptemplate warns about this restriction if you try to edit or rename these templates, and it requests confirmation before allowing you to create a new template with a .default suffix through the New, Rename or Copy functions.

Using the sptemplate utility

A template can be configured to keep repeating commands to achieve a goal such as reading output from multiple classes of sensors on an RSA II target device or reading multiple event log files one by one until no more log files exist on an iLOtype service processor. Commands may be repeated until a string, such as No more entries, is returned. When commands are repeated, an escape sequence can be used to automatically increment the number in the command, which is needed, for example, when checking event log files.

The default editor used by sptemplate is vi. You can substitute nano for vi before invoking the sptemplate utility, as shown in the following example:

```
admin@MergePoint:~# export EDITOR=/bin/nano
```

After being invoked, the sptemplate utility displays the action menu shown in the following example:

```
admin@MergePoint:~# mgp_template
Please select action:
-View
 Edit
 New
 Copy
 Rename
 Delete
 Test
 Exit
```

Selecting *New* from the Action menu brings up an editor with a template file open for you to configure.

Selecting *View*, *Edit*, *Copy*, *Test* or *Rename* from the Action menu brings up a menu of templates like the one shown in the following example:

```
Please select template to view:
-blade_center.default
 drac_mc.default
 hp_blade_system.default
 drac3.default
 drac4.default
 drac5.default
 ilom.default
 hp_ipmi.default
 rsa.default
 rsa_withoutsol.default
 ilo.default
 alom.default
 devconsole.default
 newtemplate_1
 Exit
```

If *Test* is selected, after the administrator selects a template, a list of target devices that use the selected template appears, like the list shown in the following screen example:

```
Select Service Processor to test against:


-rack1_ibm_e360_rsa_II
 rack2_ibm_e360_rsa_II
```

After the administrator selects a template and a target device to test, a list of commands to test displays like the one shown in the following example:

```
rack2_ibm_e360_rsa_II


-Access the service processor's console
 Access the device's console via SoL
 Manage power
 Reset SP
 Manage the event log - Not Supported
 View sensor output
```

```
Start Telnet session
Start SSH session
Exit
Back
```

Not all listed commands are supported on every type of target device. If you select an unsupported command, an error message displays that lists the supported commands.

The first time you select any action to test, you are prompted to enter a username and password. If local authentication is specified for the target device, enter the username and password that you entered to access the MergePoint SP manager. If another authentication method is specified for the target device, use the appropriate username and password for the specified authentication method. The test command uses the same authentication and authorization processes that the MergePoint SP manager uses in its normal operation.

See the following examples:

- The MergePoint SP manager uses local authentication, and the administrator logs into the MergePoint SP manager using the username and password pair: root/root_password.
- The administrator tests the rsa.default command template on a server called rack1_ibm_e306_rsa, which is configured for RADIUS authentication with username scottb and password cycl123. The administrator must enter scottb and cycl123 to perform the test.
- The administrator tests the rsa.default command template on a server called rack2_ibm_e306_rsa, which is configured for LDAP authentication with username sburns and password 123cycl. The administrator must enter sburns and 123cyclto perform the test.
- The administrator tests the rsa.default command template on a server called rack3_ibm_e306_rsa, which is configured for local authentication. The administrator must enter the same username/password pair that was entered to access the MergePoint SP manager (root/root_password.) to perform the test.

Each set of commands may be tested in any order after the login test is performed. Errors are generated if a command is entered out of logical order; for example, if the Reset command is issued for a server that is not powered on. After any test you can return to the editor to make changes.

While using the editor to edit, copy or create a new template, you can edit or delete fields and add comments. When the file is saved, error checking is performed. If an error is found, you are prompted either to enter the editor again to fix the error, or to discard the changes.

The following are examples of commands:

```
[rsa.default]
        type = rsa_II
        login_prompt = rname:
        pass_prompt = sword:
        cmd_prompt = [a-zA-Z0-9 #]+>
        logout_cmd = exit
```

```
        version_cmd = vpd ismp

        poweron_cmd = power on
        poweroff_cmd = power off

        powercycle_cmd = power cycle
        powerstatus_cmd = power state
        reset_cmd = reset
        sensors_cmd = {
                command = fans
                command = temps
                command = volts
        }
        sel_cmd = {
                command = readlog -f
                repeat = readlog
                until = [\n\r]*(There are no more entries in the
event log.)
        }
          clearsel_cmd = clearlog
          devconsole_cmd = console 2
          devconsole_esc = \033.
          ignore = {
                  ignore = (There are no more entries in the event
log.)[\n\r]*
          }
```

Appendix G: Advanced Boot and Backup Configuration

Boot file location

For a general description of how the MergePoint 5224/5240 appliance boots, see *Configuring boot characteristics* on page 69. If you must boot from an alternate image and the MergePoint SP manager is not available, follow the guidelines in this section. You must be an administrator and know the root password.

The MergePoint 5224/5240 appliance uses a UBoot boot loader that resides in soldered Flash memory and that automatically runs at boot time. UBoot boots the MergePoint SP manager from an image whose location is configurable. The image can reside either in a separate removable Flash memory on the MergePoint SP manager or on a boot server on the network.

NOTE: See http://sourceforge.net/projects/uboot for more information about UBoot.

The MergePoint SP manager boots from alternate images as described below.

- The MergePoint SP manager usually boots from a software image referred to as image1, which is stored on the removable Flash as an active image.
- Each time you download and install a new software version from the Avocent web site, the new image is stored as image1. The previous image is zipped and backed up as image2.
- You can choose whether the MergePoint SP manager boots from the network or the image2 (backup image) on the removable Flash.

Refer to the following text and figure partition numbers for detailed instructions about boot configuration. The first partition contains the Linux kernel, the second partition contains the rootmounted filesystem.

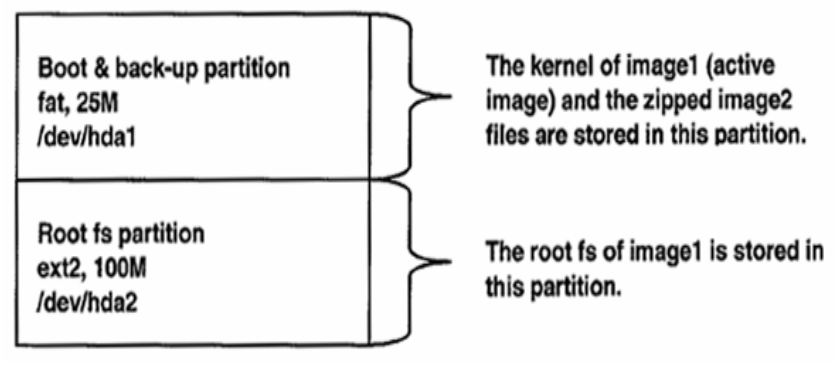

Boot & back-up partition
fat, 25M
/dev/hda1
The kernel of image1 (active image) and the zipped image2 files are stored in this partition.
Root fs partition
ext2, 100M
/dev/hda2
The root fs of image1 is stored in this partition.

Figure G.1: Partitions Layouts

Downloading a new software version

You can download a new software version in the following ways:

- Use the Web interface Upgrade Appliance Firmware screen under *System - Upgrade* to install the upgrade.
- Do a network boot from the image and then save it onto the removable Flash.

  The UBoot monitor command net_boot boots the image from the TFTP server specified in the environment variables. After the image is downloaded by network boot, the root filesystem is in the RAMDISK, and the image can run even if no removable Flash card is inserted.

  From the command line, you can then run the create_cf script with the doformat option to automatically save the image from RAMDISK into the removable Flash. The script erases everything in the Flash, partitions the Flash, if necessary, formats the partitions and copies the files currently in the RAM into the corresponding image partitions.

Changing the boot image

If you want to change to the inactive image (if there is one) from the current one, and if you have access to the web interface, you can use the Boot Configuration screen under *System - Boot Configuration* to select the image other than the current one and then apply the changes. The system will activate the selected image and then reboot into it. Meanwhile, the previous active image becomes the inactive image.

NOTE: If you cannot access the web interface, use the CLI utility.

To boot from an alternate image using CLI:

1. Connect to the MergePoint SP manager from a terminal connected to the console port or create a Telnet or SSH connection, and log in as the root user.
2. Enter the **cli** command:

   ```
   # cli
   ```

3. Enter the **get bootconf** command to check the current configuration to find out which boot image is being used.

   In the following example, image1 (the first image on the Flash card) is defined as the active image.

   ```
   cli> get bootconf
   ...
   bootconf BF_0: network
   bootconf BF_1: image1...
   bootconf BF_2: image2...
   ...
   bootconf BF_curr 1
   ```

4. Use the **set** command to change to the other image on the Flash card. Set the value of BF_curr to the index of the inactive image. For example:

   ```
   cli> set bootconf BF_curr 2
   ```

To boot from a TFTP boot server over the network:

1. Set the value of the **bootconf** command to net_boot:
   ```
   cli> set bootconf BF_curr 0
   ```
2. Set the value of the **bootconf serverip** to the TFTP boot server's IP address:
   ```
   cli> set bootconf serverip <IPaddress>
   ```
3. Set the value of the **bootconf bootfile** to be the name of the boot file on the TFTP server:
   ```
   cli> set bootconf bootfile allImage.0830 <IPaddress>
   ```
4. The current image environment variable is changed to boot from the specified image.

To boot from a TFTP server using Uboot monitor mode:

1. Boot in Uboot monitor mode.
2. Use the **setenv** command to set the ipaddr, serverip and bootfile environment variables.
   ```
   => setenv ipaddr <SPmanager_IPaddress>
   => setenv serverip <boot_server_IPaddress>
   => setenv bootfile <boot_filename>
   ```
   In the following example, the boot filename fl2222222.bin is used.
   ```
   => setenv ipaddr 192.168.45.29
   => setenv serverip 192.168.45.127
   => setenv bootfile fl2222222.bin
   ```
3. Check that the environment variables are set properly with the **printenv** command.
   ```
   => printenv
   ipaddr=192.168.45.29
   serverip=192.168.45.127
   bootfile=fl2222222.bin
   ```
4. Enter the **saveenv** command:
   ```
   => saveenv
   ```
5. Enter the **net_boot** command.
   ```
   => net_boot
   ```

UBoot network boot options and caveats

When a network boot is performed, the MergePoint SP manager boots from the specified image on the TFTP server. The image uses the RAM as the root file system. Network boots are useful for troubleshooting because the netbooted image can run even if the MergePoint SP manager's Flash memory is not usable.

Network boots are recommended only for troubleshooting and must not be used for normal operation of the MergePoint SP manager. For example, if you want to test a new release of the software to make sure a problem is fixed, or if the removable Flash memory becomes corrupted, you could download the software to a tftpboot server and save it to the removable Flash after

testing, using the create_cf command with the appropriate options (see *Reserved Words* on page 145).

To upgrade to a boot image from a network boot:

Before performing this procedure, make sure that a copy of the latest boot image has been downloaded from the Avocent ftp site to a TFTP server that is accessible to the MergePoint SP manager.

1. Boot into a network image (see *Changing the boot image* on page 142).
2. Log in as **root** after boot completes.
3. Run the **create_cf** command.

   ```
   create_cf /uImage-2.6.16 /dev/hda
   ```

CAUTION: Be aware that the create_cf command erases the Flash memory and installs the boot image into the image1 area.

4. Enter the **reboot** command to restart the unit.

   ```
   root@MergePoint:~# reboot
   ```

Appendix H: Reserved Words

Reserved words are predefined words that have special meaning to the MergePoint SP manager. Do not use the following reserved words when configuring usernames.

Table H.1: Reserved Words

Reserved Words (Do Not Use as Usernames)								
adm	bin	disk	irc	man	proxy	sudo	utmp	www-data
admin	cdrom	fax	kmem	news	root	sync	uucp	
apache	daemon	floppy	list	nobody	shadow	sys	video	
audio	dialout	games	lp	operator	src	tape	voice	
backup	dip	gnats	mail	postgres	sshd	tty	wheel	

Appendix I: Glossary and Acronyms

BMC

The Baseboard Management Controller (BMC) is a specialized micro-controller on an IPMI target device that monitors and logs environmental conditions, such as temperature, voltage and power supply.

CIM

Common Information Model (CIM), developed by DMTF, is a common data model of a schema used to describe overall management information in a network or enterprise environment.

Client PC

The client PC is a remote user workstation that is currently running the MergePoint SP manager web interface through a browser.

DMTF

The Distributed Management Task Force (DMTF) is a not-for-profit association promoting enterprise and systems management and interoperability. Visit www.dmft.org for more information.

DRAC

The Dell Remote Access Card (DRAC) is an intelligent service processor integrated on certain Dell target devices. DRAC III and IV target devices are supported by the MergePoint SP manager.

iLO

Integrated Lights-Out (iLO) is an intelligent service processor integrated on certain Hewlett Packard (HP) target devices. iLO target devices are supported by the MergePoint SP manager.

IPMI

Intelligent Platform Management Interface (IPMI) defines a set of common interfaces to computer hardware and firmware. System administrators may use IPMI to monitor system health and manage a system with an IPMI BMC. Target devices with IPMI BMCs are supported by the MergePoint SP manager.

MOF

Managed Object Format (MOF) is a data structure used by CIM to describe all managed targets on the network.

PET

Platform Event Trap (PET) is a specific format of SNMP trap used for system management alerts.

SSH

Secure Shell (SSH) is a UNIX-based command interface and protocol that allows administrators to securely access a remote target device.

SoL

With Serial over LAN (SoL), the serial console output of a device is redirected over IP, providing access to text-based interfaces for BIOS, utilities, operating systems and applications and to service processor functions.

Target device

A target device can be a data center component such as a server or router that an administrator can remotely manage through the MergePoint SP manager.

Telnet session

A Telnet session is a type of target device session. Once the MergePoint SP manager appliance is set up, a user may connect directly to a target device using Telnet and manage the target device using SMASH CLP commands.

Unit

Unit refers to the MergePoint SP manager. A device being managed by the appliance is referred to a target or a target device.

WBEM

WBEM stands for Web Based Enterprise Management. WBEM is a set of management and Internet standard technologies developed by DMTF to unify the management of distributed computing environments.

Appendix J: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service.

To resolve an issue:

1. Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.
2. Visit www.avocent.com/support and use one of the following resources:

   Search the knowledge base or use the online service request.
   -or-
   Select *Technical Support Contacts* to find the Avocent Technical Support location nearest you.

License Information

This product includes various software programs that are copyrighted and released under the GNU General Public License (GPL), the GNU Lesser General Public License (LGPL), and other licenses that permit copying, modification, and redistribution of source code (such licenses referred to as Public Licenses), in particular the software program "mtd". A machine-readable copy of the source code protected by these Public Licenses is available from Avocent on a medium customarily used for software interchange for a period of three years from date of purchase of this product by contacting Avocent Corporation at www.Avocent.com/support. AVOCENT CORPORATION AND ITS LICENSORS MAKE NO WARRANTY (EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE) OF ANY KIND REGARDING THE SOFTWARE PROGRAMS LICENSED UNDER ANY PUBLIC LICENSE, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AVOCENT CORPORATION AND ITS LICENSORS DISCLAIM ANY AND ALL OTHER WARRANTIES AND CONDITIONS WITH RESPECT TO THE SOFTWARE PROGRAMS LICENSED UNDER ANY PUBLIC LICENSE.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free

redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

For Technical Support:
www.avocent.com/support

590-765-501B